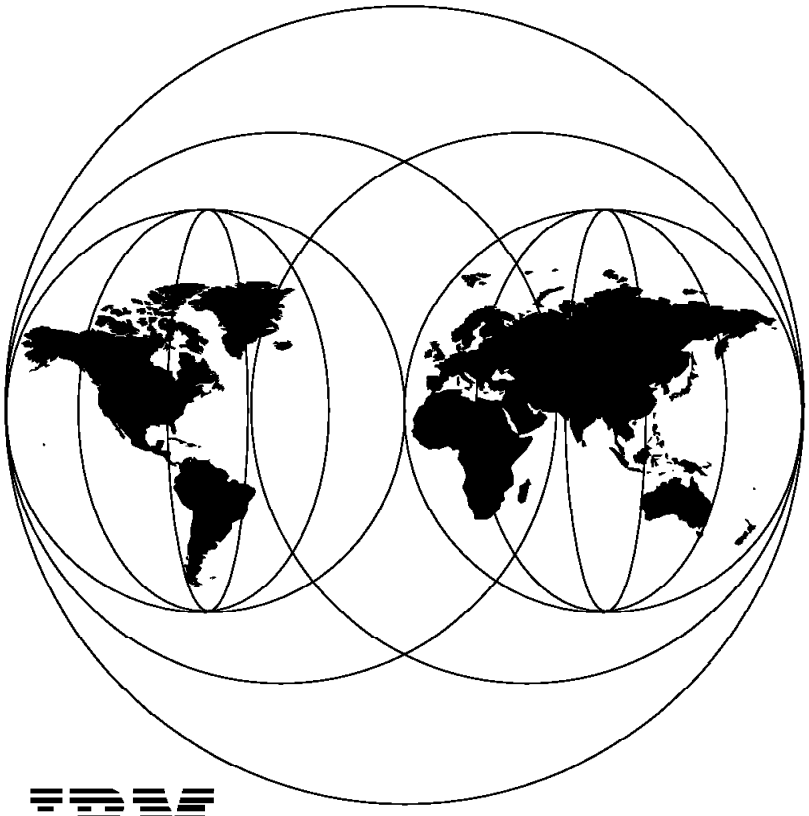
SG24-4723-00

Systems Management from an NT Server Point of View

September 1996



IBM

International Technical Support Organization
Raleigh Center

International Technical Support Organization

SG24-4723-00

Systems Management from an NT Server Point of View

September 1996

Take Note!

Before using this information and the product it supports, be sure to read the general information in Appendix D, “Special Notices” on page 175.

First Edition (September 1996)

This edition applies to V4.0 of TME 10 NetFinity, Part Number 78H5375 and 78H5376 for use with the NT V3.51 Server Operating System.

Comments may be addressed to:
IBM Corporation, International Technical Support Organization
Dept. HZ8 Building 678
P.O. Box 12195
Research Triangle Park, NC 27709-2195

When you send information to IBM, you grant IBM a non-exclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

© **Copyright International Business Machines Corporation 1996. All rights reserved.**
Note to U.S. Government Users — Documentation related to restricted rights — Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract with IBM Corp.

Contents

Preface vii
How This Redbook Is Organized vii
The Team That Wrote This Redbook viii
Comments Welcome viii

Chapter 1. TME 10 NetFinity Overview 1
1.1 What Is TME 10 NetFinity under NT 1
1.2 Hardware and Software Requirements under NT 1
1.3 Installation under NT 3
1.3.1 Installation of TME 10 NetFinity Services 3
1.3.2 Installation of a TME 10 NetFinity Manager 6
1.4 TME 10 NetFinity Configuration 7
1.5 Hints and Tips 10

Chapter 2. NT Systems Management Functions 11
2.1 System Management Functions Provided by TME 10 NetFinity 11
2.1.1 TME 10 NetFinity Functions for Services 12
2.1.2 TME 10 NetFinity Functions for Manager 39
2.2 System Management Functions Provided by Windows NT 54
2.2.1 Windows NT Disk Administrator 54
2.2.2 Windows NT Performance Monitor 56
2.2.3 Windows NT Server Manager 58
2.2.4 Windows NT Event Viewer 59
2.2.5 Windows NT Diagnostics 60
2.2.6 Windows NT Registry Editor 61
2.2.7 Windows NT Dr. Watson Utilities 64
2.2.8 Windows NT License Management 65
2.2.9 Windows NT Replication Service 70
2.3 System Management Tools Provided by Windows NT Resource Kit 74
2.3.1 Automatic Login and Shutdown Management 77
2.3.2 Process Management 80
2.3.3 Performance Monitoring 82
2.3.4 Command Scheduler 84
2.3.5 Network and Domain Monitoring 86
2.3.6 Windows NT Setup Manager 90

Chapter 3. Alert Flows 95
3.1 Alerts by TME 10 NetFinity 95
3.1.1 Alert Manager 95
3.2 View Alert Log 96
3.2.1 Alert Forwarding and Alert Flow 96
3.2.2 Alert Profiles 99
3.2.3 Severity 100
3.2.4 Alert Actions 100
3.2.5 Command Line Interface 102
3.2.6 Applications Sending Alerts to the Alert Manager 104
3.3 Alerts by Windows NT Performance Monitor 114
3.3.1 Alert Generating 114
3.3.2 Alert Forwarding 116

Chapter 4. Managing Clients 117

© Copyright IBM Corp. 1996

4.1 Installation and Configuration . . . 117
4.1.1 Windows 3.1 and Windows 95 Installation . . . 117
4.1.2 NetWare Installation . . . 117
4.2 Functions and Differences . . . 118
4.2.1 Windows 95 and Windows 3.11 . . . 118
4.2.2 OS/2 Warp . . . 118
4.2.3 NetWare . . . 118
4.3 Summary . . . 119

Chapter 5. TME 10 NetFinity Database Support . . . 123
5.1 Database Support with ODBC Drivers . . . 124
5.2 TME 10 NetFinity with IBM DB2 for Windows NT Using ODBC . . . 124
5.2.1 Setup DB2 for Windows NT and Create Database . . . 124
5.2.2 Install and Configure DB2 ODBC Support . . . 125
5.2.3 Create TME 10 NetFinity Tables through the ODBC Driver . . . 127
5.3 TME 10 NetFinity with Microsoft SQL Server Using ODBC . . . 130
5.3.1 Setup Microsoft SQL Server and Create Database . . . 130
5.3.2 Install and Configure Microsoft ODBC Support . . . 138
5.3.3 Create TME 10 NetFinity Tables through the ODBC Driver . . . 139
5.4 TME 10 NetFinity with Direct Access to the IBM DB2 NT Database . . . 140
5.5 Export Data from TME 10 NetFinity to Database . . . 140
5.6 Query the TME 10 NetFinity Database . . . 143

Chapter 6. Webability . . . 145
6.1 Internet Connections to TME 10 NetFinity . . . 145
6.1.1 Accessing Remote LANs Using an Internet Server on the Remote Site . . . 147
6.1.2 Accessing Remote LANs Using a Service Provider . . . 149
6.1.3 Accessing Remote LANs Using an Internet TCP/IP Address . . . 150
6.2 Configuration of the Web Manager . . . 151
6.3 Internet Client Functions . . . 153
6.3.1 Limitations When Using the Web Manager . . . 164

Appendix A. Application Alerts and Alert IDs . . . 167

Appendix B. List of Supported Modems . . . 169

Appendix C. TME 10 NetFinity Monitors . . . 171
C.1 OS/2 System Monitors . . . 171
C.2 Windows NT Monitors . . . 171
C.3 NetWare 3.x/4.x Monitors . . . 172
C.4 Windows 3.x and Windows 95 Monitors . . . 172
C.5 Monitors Provided by NetFinity Partners . . . 172
C.5.1 APC (American Power Conversion) . . . 172
C.5.2 Lexmark International . . . 172
C.5.3 BMC Software . . . 173

Appendix D. Special Notices . . . 175

Appendix E. Related Publications . . . 177
E.1 International Technical Support Organization Publications . . . 177
E.2 Redbooks on CD-ROMs . . . 177
E.3 Other Publications . . . 177

How To Get ITSO Redbooks . . . 179

How IBM Employees Can Get ITSO Redbooks 179
How Customers Can Get ITSO Redbooks 180
IBM Redbook Order Form 181

Index 183

Preface

This redbook is unique in its detailed coverage of systems management on the NT operating system. In addition, its main focus is on using the IBM systems management tool, TME 10 NetFinity. It provides information on built-in tools that come with NT Server V3.51 as well as the NT Resource Kit. It also shows how to manage from the NT operating system using a new Web browser interface.

This redbook was written for systems managers who work on the NT platform and wish to know more about TME 10 NetFinity and other NT systems management functions.

Several practical examples are presented to demonstrate the integration of the NT operating system with TME 10 NetFinity and the NT Resource Kit. Some knowledge of NT Server and any version of NetFinity or TME 10 NetFinity is assumed.

How This Redbook Is Organized

The redbook is organized as follows:

- Chapter 1, “TME 10 NetFinity Overview”

  This chapter provides an overview of TME 10 NetFinity on the NT operating system. It shows how to install the product and configure it.

- Chapter 2, “NT Systems Management Functions”

  This chapter provides an overview of the built-in functions of the NT operating system that a systems manager would be interested in. In addition, it shows the functions that are added with the NT Resource Kit.

- Chapter 3, “Alert Flows”

  This chapter describes how alerts are managed with TME 10 NetFinity. The life cycle of an alert is shown, from how to create an alert to how to process it.

- Chapter 4, “Managing Clients”

  This chapter provides examples of how to install and use TME 10 NetFinity clients on all the supported platforms.

- Chapter 5, “TME 10 NetFinity Database Support”

  This chapter provides a description of how to integrate database support into TME 10 NetFinity. The focus of this chapter is on how to set up the databases and export data to them.

- Chapter 6, “Webability”

  This chapter provides examples of how to use the new Webability feature that comes with this new release of TME 10 NetFinity.

- Appendix A, “Application Alerts and Alert IDs”

  This appendix describes alerts that are provided with TME 10 NetFinity.

- Appendix B, “List of Supported Modems”

  This appendix describes modem settings for serial connections.

- Appendix C, “TME 10 NetFinity Monitors”

© Copyright IBM Corp. 1996

This appendix provides a list of the monitors that are available with TME 10 NetFinity on all platforms.

The Team That Wrote This Redbook

This redbook was produced by a team of specialists from around the world working at the Systems Management and Networking ITSO Center, Raleigh.

Barry D. Nusbaum is a Senior International Technical support representative at the Systems Management and Networking ITSO Center, Raleigh. He writes extensively and teaches IBM classes worldwide on all areas of TME systems management on the NT and AIX platform. Before joining the ITSO 4 years ago, Barry D. Nusbaum worked in Professional Services in the United States as the National Communications Specialist.

Christian Jaeggli is a systems specialist in Switzerland. He has several years of experience in systems management.

Manfred Schneider is a systems specialist in Germany. He has several years of experience in systems management.

Thanks to the following people for their invaluable contributions to this project:

Tim Kearby
Systems Management and Networking ITSO Center, Raleigh

David Young and Wade Mahan
IBM RTP

Benjamin Reed and Steve Welch
IBM Almaden

Comments Welcome

We want our redbooks to be as helpful as possible. Should you have any comments about this or other redbooks, please send us a note at the following address:

redbook@vnet.ibm.com

Your comments are important to us!

Chapter 1. TME 10 NetFinity Overview

This chapter provides an overview of the TME 10 NetFinity product, as well as shows the installation and configuration of TME 10 TME 10 NetFinity on the NT platform. This includes the hardware and software requirements.

1.1 What Is TME 10 NetFinity under NT

TME 10 NetFinity is a set of applications used for systems management and monitoring capabilities. Due to its product structure, it is very flexible and allows updating of existing product components new features without having to reinstall the product.

TME 10 NetFinity enables you to monitor and manage systems locally and remotely without any interruptions to your users. It helps keep you informed about actual problems within your network as well as helping you to fix them. It is also very flexible when it comes to connecting to its clients. From a functional perspective, the transport protocol used for connectivity does not determine which services are available. When connecting to its clients, it uses just the network device drivers, which makes it very convenient if you want to change the network adapters. You don′t have to make any changes within TME 10 NetFinity if you change transport protocols, just the operating system device drivers.

TME 10 NetFinity is designed to help solve problems for your clients whether their workstations are notebooks, desktops or servers as long as the workstations are systems that are running under the TME 10 NetFinity-supported operating systems.

TME 10 NetFinity is part of the TME 10 product family, which also means that it will cooperate with all the other SystemView products on the MVS, AIX and OS/400 platforms as well as with other TME 10 products.

This redbook describes the systems management capabilities of TME 10 NetFinity on NT Server 3.51 as well as the systems management functions that are built into the NT operating system. In addition, we use the NT 3.51 Resource Kit to extend the systems management functions. We show how to manage clients that are on the Windows NT, Windows 95, NetWare and OS/2 platforms. This redbook also shows the different facilities of TME 10 NetFinity available under NT in conjunction with TME 10 NetFinity on other TME 10 operating systems as well as the Windows NT 3.51 Advanced Server system management functions built into the server software.

1.2 Hardware and Software Requirements under NT

1. Software requirements:
   - Operating System:
     - Microsoft Windows NT 3.x
     - OS/2 2.11 or higher
     - DOS Windows 3.11
     - Windows 95

© Copyright IBM Corp. 1996

- Novell NetWare 3.1x or higher

- TME 10 NetFinity Version 4.0 (Services or Manager)

2. Hardware requirements:

   - Personal computer with at least a 80386 processor, depending on the operating system used for this workstation.
   - 7 - 10 MB (Services); 12-15 MB (Manager) - available hard disk space
   - At least one LAN adapter with one of the following communications protocol drivers installed:
     - NetBIOS

       At least two names, one session and five NCBs are required for NetBIOS.
     - IPX
     - IBM TCP/IP for DOS or another WinSock Version 1.1 compatible driver

3. Connection possibilities for TME 10 NetFinity:

   There are different ways to connect your TME 10 NetFinity manager to your workstations. Also, several operating systems and communication protocols are supported. See Figure 1 on page 3 for an overview of these connections.

   - You can use any hardware connection to your clients and servers as long as you provide a supported network device driver. This may be a connection on a LAN such as a token-ring or Ethernet or a WAN connection using LAN distance or bridges and routers depending on the protocols that are used.
   - You also may use a serial connection for your access. See Chapter 2, “NT Systems Management Functions” on page 11 for details on the configuration for this type of connection. A lot of different modems have been pre-configured in TME 10 NetFinity to make the integration easier. In Appendix B, “List of Supported Modems” on page 169 you will find a complete list of the already pre-configured modems supported by TME 10 NetFinity. Of course you can modify and add any additional definitions for your own modems.
   - Another way to connect to your remote workstations is to use the Internet. We provide an easy-to-use interface to manage remote clients over the WWW. See Chapter 6, “Webability” on page 145 for details on the new Internet service.

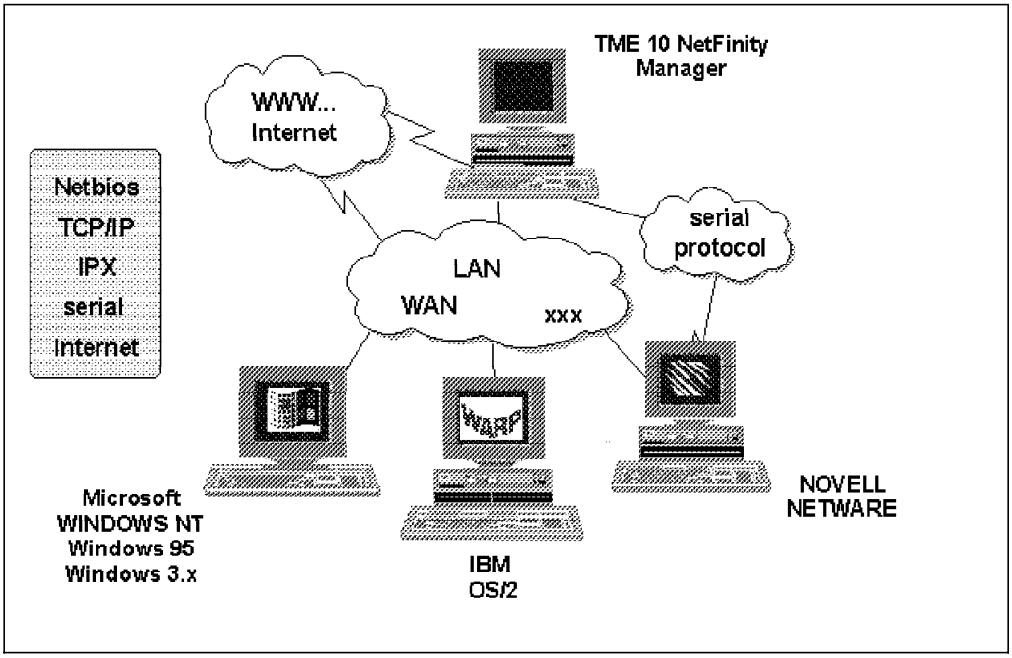


Figure 1. TME 10 NetFinity Connections

1.3 Installation under NT

In this section we describe how to install TME 10 NetFinity under Windows NT as a manager, as well as a client.

The TME 10 NetFinity for NT consists of a package of five diskettes or one CD. You first have to decide whether you want to install the TME 10 code as *services* or *manager*. On the CD-ROM you will find the code in different subdirectories. The diskettes are labeled *TME 10 NetFinity Services* or *TME 10 NetFinity Manager*. The services code is just for the clients and the TME 10 NetFinity manager code is for managing workstations.

1.3.1 Installation of TME 10 NetFinity Services

1. Insert the first diskette for the TME 10 NetFinity Services.
2. Go to an MS-DOS command prompt and type:

   ```
   A:\NETFINST
   ```

   This results in execution of the installation program for TME 10 NetFinity.
3. A window will pop up indicating a default drive and directory where you install the code. You can override the default by typing in a new location (see Figure 2 on page 4). The installation can be from a diskette, CD or a LAN drive. The same applies to the target drive. You should also define the subdirectory where the code will be installed.
4. After you have defined the source and target drives you now have to define the type of TME 10 NetFinity client you want to install. There are different types of clients that can be installed. Figure 3 on page 4 shows the installation options.

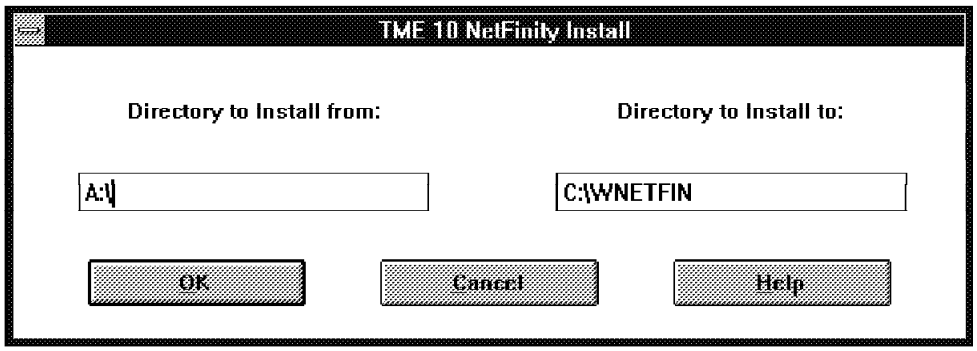


Figure 2. Drive Selection for TME 10 NetFinity Installation

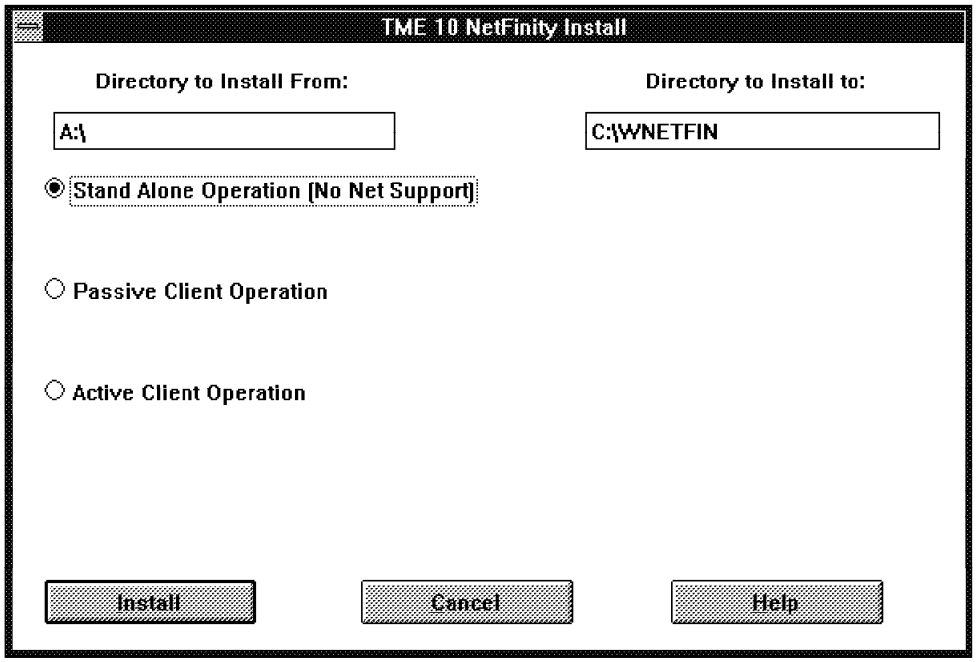


Figure 3. Choice of Client User Interface

5. The following are the different types of clients that you can install. Figure 3 depicts what the options are.

   - Stand-alone client

     The stand-alone client can only perform TME 10 NetFinity functions locally and has no network interface support installed. This means that the network administrator has no access to this workstation over the LAN using TME 10 NetFinity.

   - Passive client

     The passive client can't perform most of the TME 10 NetFinity functions locally. Only the TME 10 NetFinity services for the alert, security manager and for the serial control are available. For the other services it can only respond and react to requests from a TME 10 NetFinity manager. See Figure 4 on page 5 for the user interface for this client.

     The following figures represent the services available at the client, depending upon which type of client you have installed.

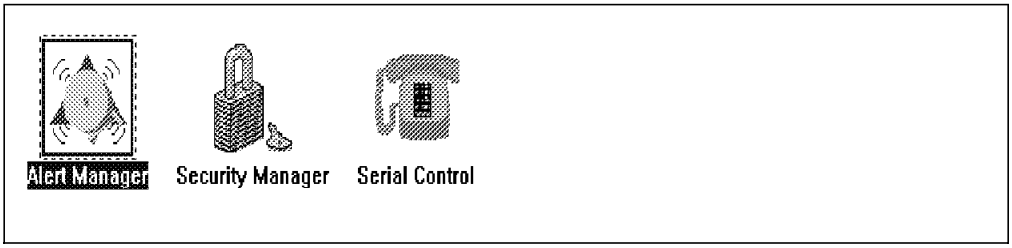


Figure 4. Passive Client User Interface

- Active client

  The active client can perform all TME 10 NetFinity Services locally. See 2.1.1, " TME 10 NetFinity Functions for Services" on page 12 for a complete list of available functions. It also can react to requests from a TME 10 NetFinity manager over the LAN. Also see Figure 5 for the user interface of this client.

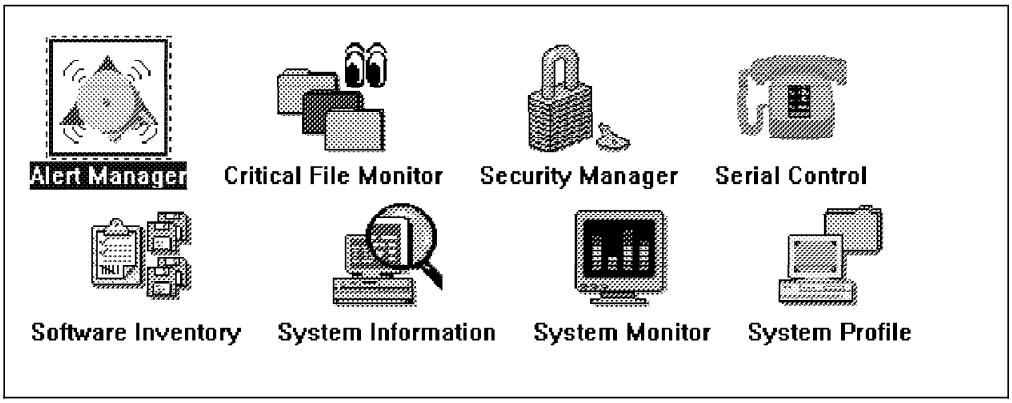


Figure 5. Active and Stand-Alone Client User Interface

6. You now see a window that shows you the actual status of the installation in progress (see Figure 6 for details). In case of an installation from diskette you are now prompted during the installation process for additional diskettes.

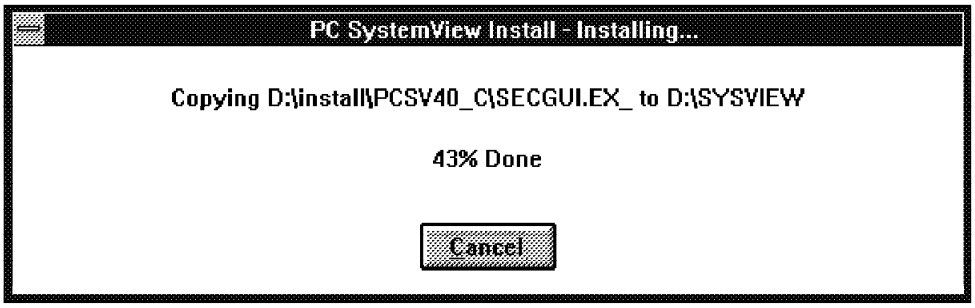


Figure 6. Installation in Process

7. After installing the code from the TME 10 NetFinity Services diskettes you are prompted for the configuration of the TME 10 NetFinity client. This definition is described in detail in 1.4, "TME 10 NetFinity Configuration" on page 7. Figure 9 on page 8 shows the configuration menu.

1.3.2 Installation of a TME 10 NetFinity Manager

To install the TME 10 NetFinity Manager code on your workstation you have to insert the first manager diskette and also start the *NETFINST* program from this diskette. The installation of the TME 10 NetFinity Manager after this is very similar to the services installation except that instead of being asked for the type of client, you are asked whether you want to use your manager with Web Enhancement support or without it. See Figure 7 for the definition menu. The rest of the installation actions are the same as in the services installation. The functions of the Webability support are described later in Chapter 6, “Webability” on page 145.

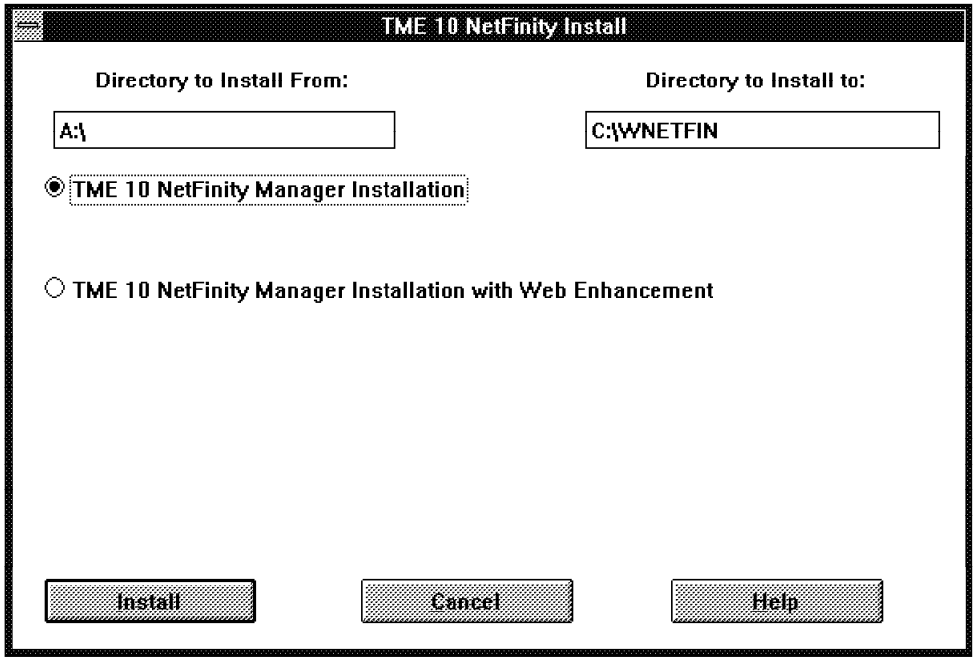


Figure 7. Installation Options for the TME 10 NetFinity NT Manager

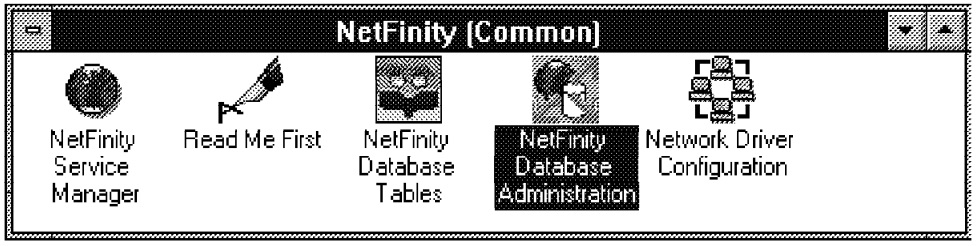


Figure 8. TME 10 NetFinity Folder for Manager

The TME 10 NetFinity folder for managers as seen in Figure 8 includes the following services:

- NetFinity Service Manager

  The TME 10 NetFinity Manager gives you the management functions provided by TME 10 NetFinity. When started, it will provide the interface that provides the graphical user interface for the TME 10 NetFinity services. The detailed description of the functions can be found in Chapter 2, “NT Systems Management Functions” on page 11.

- Read Me First

  This is a typical readme file, that provides some hints and tips as well as some general information on TME 10 NetFinity.

- TME 10 NetFinity Database Tables

  If you select this function you will get detailed information on how the database tables, created by TME 10 NetFinity, are structured. This might be very useful, if you create your own databases and want to include the TME 10 NetFinity information in that database. More details about the databases and their structure can be found in Chapter 5, “TME 10 NetFinity Database Support” on page 123.

- TME 10 NetFinity Database Administration

  The administration functions are used to define what kind of database is being used. You may select IBM DB2 using ODBC or MS SQL Server using ODBC.

- Network Driver Configuration

  This is very important. You have to be careful with the configuration done in the network driver configuration. The detailed menu can be seen in Figure 9 on page 8. It is used to define the possible connections for the TME 10 NetFinity workstations.

1.4 TME 10 NetFinity Configuration

In this section we describe how the configuration of the services and managers are done and also explain the contents of the fields that are in Figure 9 on page 8.

The main configuration menu within the TME 10 NetFinity configuration is the Network Driver Configuration menu which is shown in Figure 9 on page 8. The network configuration menu will automatically show up at the end of the installation process, so you are able to check and correct your network support definitions for TME 10 NetFinity. You can also change it at any time by double-clicking on the **Network Driver Configuration** icon in the NetFinity common window on the desktop.

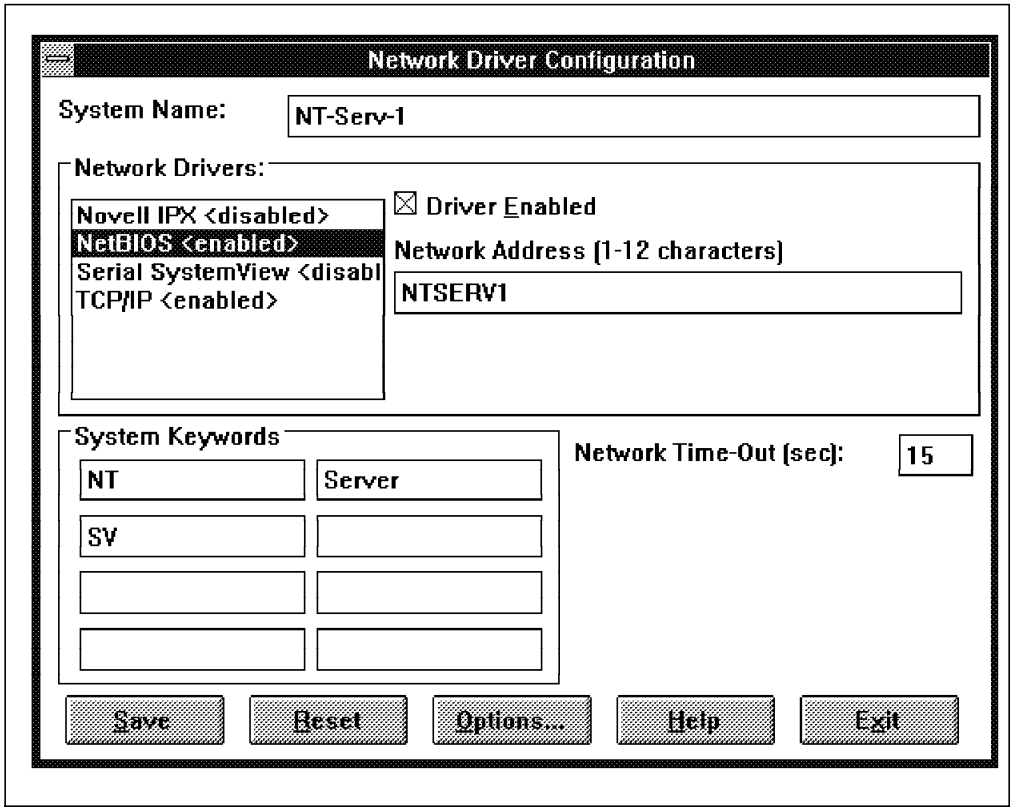


Figure 9. Network Driver Configuration

The main purpose of the network driver configuration is to define the connections to and from the other workstations using TME 10 NetFinity. Let's have a look at the following definition fields within this menu and their meanings:

- System Name

  The System Name field can be any combination of alphanumeric characters including blanks. It shows the name of the workstation. This name can be seen later in the management process when monitoring the client groups. It is used to easily identify your workstations.

- Network Drivers

  The Network Drivers field automatically shows you all the installed network device drivers such as NetBIOS, IPX, TCP/IP and Serial support. In parentheses you can find the status of this driver, which means, whether or not this driver has been activated for TME 10 NetFinity usage. You can easily activate or deactivate any of the drivers by selecting it with the mouse and marking the check box Driver Enabled. If TME 10 NetFinity is running, you will need to restart it to add the additional protocols. The Network Driver Configuration panel is shown in Figure 9. In this menu you can see that the NetBIOS and TCP/IP drivers are enabled, which means they can be used by TME 10 NetFinity. The IPX and SERIAL driver support are installed, but disabled. In this example we selected the NetBIOS driver (highlighted) and marked the Driver Enabled check box. The Network Address field shown in this figure shows some additional required information depending on the device driver. For NetBIOS this will be a NetBIOS name which is used for communication between the manager and its clients.

- System Keywords

The system keywords are not required for TME 10 NetFinity, but it makes life easier for the network administrators. They are used to identify and group the workstations and servers within the network. If you are running in a stand-alone environment, these keywords won't be used. The keywords are used within a network environment to identify and define groups among the workstations. This is explained in more detail in Chapter 2, "NT Systems Management Functions" on page 11 when we describe the way to define groups and the functions that can be performed for entire groups.

- Network Time-Outs

  This defines the timeout interval before you get an error message when you try to use one of the remote functions of TME 10 NetFinity.

Within the driver configuration menu you can also see an Options selection button. If you select this, an Option Definition menu is shown (see Figure 10 on page 10).

1. Force Remote Logons

   If you are accessing remote workstations as a TME 10 NetFinity Manager, you can choose to save a user ID and a password for the different workstations. The next time you access the same workstation TME 10 NetFinity will automatically provide the same user ID and password that was specified on your first connection. This might be risky, because if somebody else gets access to your managing workstation, they can access your clients without providing a user ID and password. So there might be a chance of violating the security. If you select Force Remote Logons, you are not able to save the user ID and password. Therefore, every time you access another workstation you will be prompted to provide a user ID and a password.

2. Service Execution Alerts

   Whenever a TME 10 NetFinity manager accesses your workstation, TME 10 NetFinity will send an alert. This is true for every access of the TME 10 NetFinity services. An alert will be created with the information about who is using one of the TME 10 NetFinity services on your workstation. You can then decide what you want to do about it. This can be done using an EXEC to take some specific action using the alert editor, or something as simple as providing a pop-up window.

3. Show Support Program

   The Show Support Program function is only available on Windows 3.1, Windows for Workgroups, Windows 95 and Windows NT workstations. In NetWare and OS/2 this function is automatically enabled and you can't de-select it. This function lets the TME 10 NetFinity support program run in a visible session, so that you are able to shut down the TME 10 NetFinity support program. If you don't want to have it visible, so that your users cannot shut down the TME 10 NetFinity support program, don't enable this function. Disabling this function is probably a good idea on client workstations so that the users do not shut down the TME 10 NetFinity client by mistake and hinder the problem determination process.

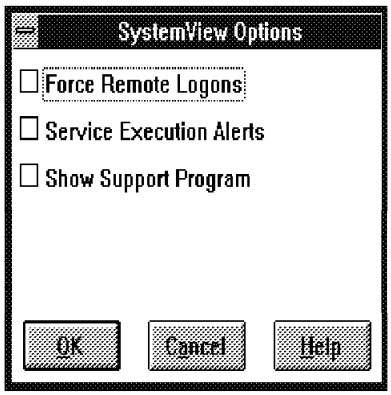


Figure 10. Driver Configurations Options

After you have finished your installation as a TME 10 NetFinity manager and you have rebooted your system once to activate the device drivers you will see the following window. You now may use the different functions of TME 10 NetFinity.

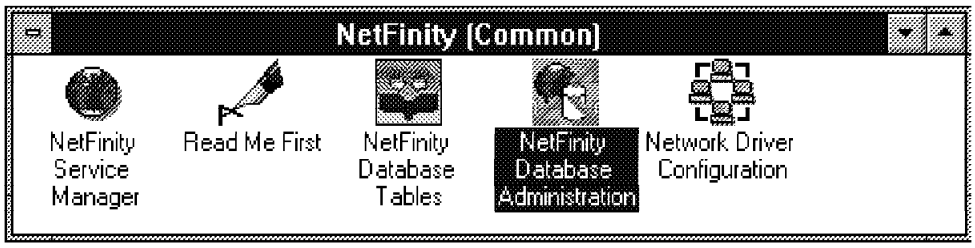


Figure 11. TME 10 NetFinity Service Manager

1.5 Hints and Tips

We didn't experience any major problems during the installation and configuration of this product. However, the following are some hints, which might be of interest to you:

1. Make sure that the network drivers have been installed before installing TME 10 NetFinity, otherwise you will not be able to define the appropriate network connection during the installation process and you will have to do it later on.
2. Think about defining Force Remote Logon for security reasons, so that nobody else who might not be authorized can access any other workstations.
3. Don't forget to define the Security service for each workstation. You will find a detailed description on how to do this and what to take care of during this process in Chapter 2, "NT Systems Management Functions" on page 11.
4. It might also be useful to define Show Execution Alerts within the Network Driver Configuration Options menu. This enables your users to monitor the network administrator actions when accessing the users workstation. The information from these actions may also be logged in the alert log. If any problem occurs later on then there is a chance that you can tell who accessed the workstation, what services they tried to use and what the problem might be.

Chapter 2. NT Systems Management Functions

This chapter shows examples of TME 10 NetFinity for NT systems management functions, as well as built-in systems management functions of NT.

2.1 System Management Functions Provided by TME 10 NetFinity

Within this chapter we describe all the different TME 10 NetFinity functions available under NT with the appropriate definitions and menu descriptions. There are two different products available for TME 10 NetFinity.

1. TME 10 NetFinity Services

   TME 10 NetFinity Services should be installed on all clients to provide both local TME 10 NetFinity support as well as to enable remote TME 10 NetFinity functional support. Enabling remote support means that it will respond to the requests of the manager and send the requested information to the manager workstation. TME 10 NetFinity Services will not let you access other workstations to do management functions. You will need to be a manager to do that.

2. TME 10 NetFinity Manager

   TME 10 NetFinity Manager needs to be installed if remote access to the workstations or servers is required in the case of systems management. It is also possible to run all functions locally or remotely and request all information from a remote workstation. The TME 10 NetFinity Manager product is a combination of the NetFinity Services and Manager product.

When using a Windows NT 3.51 server noone has to be logged on at the server itself for the NetFinity services functions to be active. For example, this means that the time and date controlled services using the event scheduler can run, even if nobody is logged on. Also the NT server′s NetFinity services may be accessed by another TME 10 NetFinity Manager over any transport protocol, even if no one is logged on. It can also be done over an intranet or the Internet using the Webability feature of TME 10 NetFinity as discussed in Chapter 6, “Webability” on page 145. The TME 10 NetFinity network interface (NETFBASE.EXE) is automatically started and becomes active during the Windows NT 3.51 startup with all the transport protocols that were defined in the driver configuration.

© Copyright IBM Corp. 1996

2.1.1 TME 10 NetFinity Functions for Services

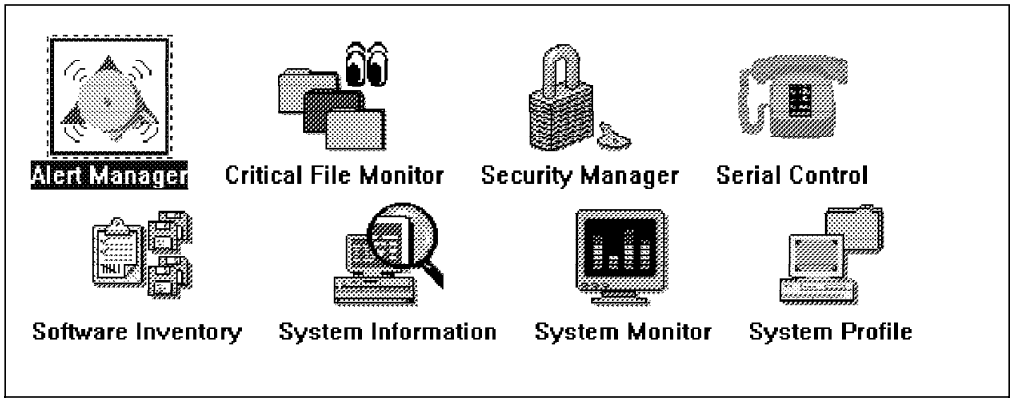


Figure 12. TME 10 NetFinity Services

In the above picture you can see the functions that are available if you install TME 10 NetFinity Services. It is limited to local functions within your workstation. Of course you may also use the same functions as a manager locally. For additional remote functions, see 2.1.2, " TME 10 NetFinity Functions for Manager" on page 39.

2.1.1.1 System Information

Figure 13. System Information Service

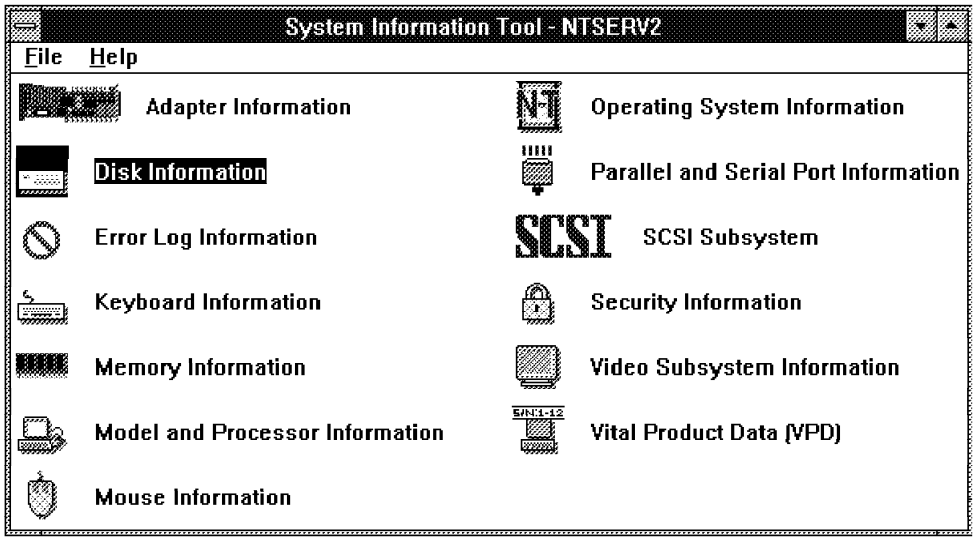


Figure 14. System Information

The System Information facility is used to gather information about the hardware and software configuration of the workstations. The amount and the depth of the

details of the information which can be retrieved depends on the hardware and software that is installed. For example, if you have an AT bus-based system installed, then you cannot get any detailed adapter information from this system, because the hardware architecture does not provide you with these details. However, you may use this service on any personal computer, independent of the brand it is. Note, that with some equipment there may be some limitations as to the information that is gathered by this service. An example of this follows:

- Adapter Information

  Selecting this gets you detailed information on the currently installed adapters in this system. A more detailed description can be found in the section below as an example of what kind of information can be retrieved and what the information looks like.

- Error Log Information

  Selecting this retrieves the actual hardware error log.

- Keyboard Information

  Selecting this gives you detailed information on the type and layout of the connected keyboard.

- Memory Information

  The details of this information depend on the type of system. Normally when you select this you will get information on the amount of memory, the type of memory, SIMM type and the number of SIMMs. Depending on the system it may also show you a list of SIMM types, which are supported in this workstation.

- Model and Processor Information

  You will get information like processor type, speed and possibly information about the manufacturer and system type when you choose this.

- Mouse Information

  The type of the installed mouse is given when you click on this.

- Operating System Information

  You can find the following information about the installed operation system when you select this:

  - Operating system details, which show you the type of operating system such as Windows NT, OS/2, NetWare, Windows 95 and information about the version and boot drives.
  - Service level information like the CSD level of all OS/2 components.
  - Window list, which gives you the details of what currently is running on this workstation in the foreground or hidden applications that might be running in the background.
  - CONFIG.SYS contents of the workstation and also file information about the drivers that have been loaded by this CONFIG.SYS. For example, it gives you the size, time and date information for the LAN device driver.

- Parallel and Serial Port Information

  You will get details about the defined logical and physical serial and parallel connections and their supported transfer rates when you select this.

- Disk Subsystem, which in our case was a SCSI subsystem

Selecting this provides you with information on the hard disk controller and its definition as well as information on the connected hard drives and other drives that are also connected to the same controller. An example of this could be a CD-ROM.

- Security Information

  Selecting this gives you details about the installed hardware security features.

- Video Subsystem Information

  Selecting this gives you details on attached screen information and also about the graphics controller such as supported resolution, memory.

- Vital Product Data (VPD)

  This only applies if your system offers VPD data. This might be software and hardware related. Normally this is information such as type and serial number of the system as well as maintenance information on the components (for example, EC level of the system board).

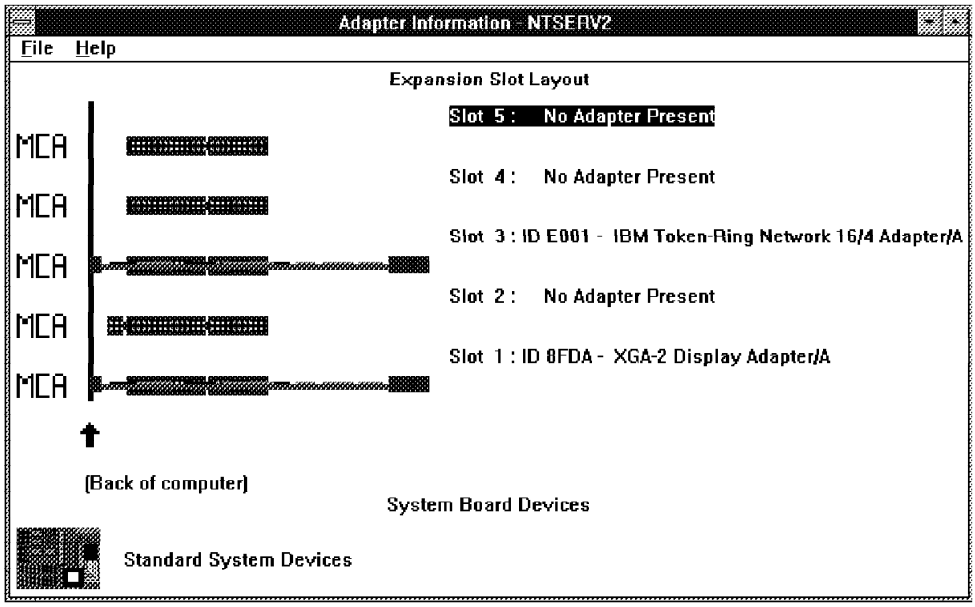


Figure 15. Slots and Adapter

If you have selected Adapter Information on the previous screen, then you will get detailed information on the adapters, which are currently installed in this system. In our case these are all Micro Channel adapters. As you can see, there is an IBM Token-Ring 16/4 adapter installed in slot 3 and an XGA adapter installed in slot 1. The other slots are not used at this time. If you now want to get more detailed information on one of these adapters, then double-click on the slot display of the adapter you want to get more details on. Then an additional menu gives you very detailed information about the configuration data for this adapter, such as interrupts, memory on the adapter, transfer rates.

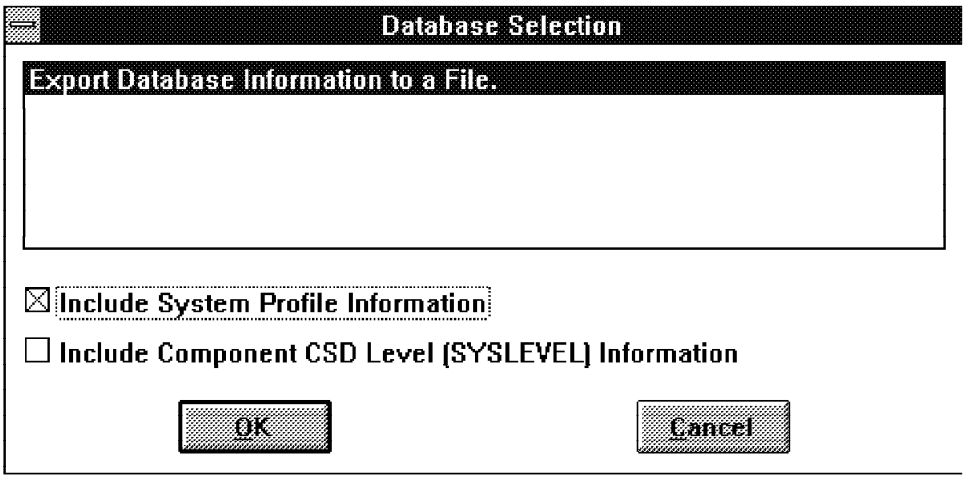


Figure 16. Database Selection

In addition, you can transfer all information from the System Information Service to a database. Figure 16 shows the format of the definition and that it is possible to also include the System Profile Service Information, which will be discussed in 2.1.1.2, “System Profile Service.” Within 5.5, “Export Data from TME 10 NetFinity to Database” on page 140 you can find more details about how this database looks and how to export this data to the database. There is also a lot of information about the different database formats.

2.1.1.2 System Profile Service

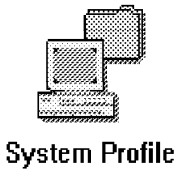


Figure 17. System Profile Service

The system profile service can be used to add personal information to the inventory data.

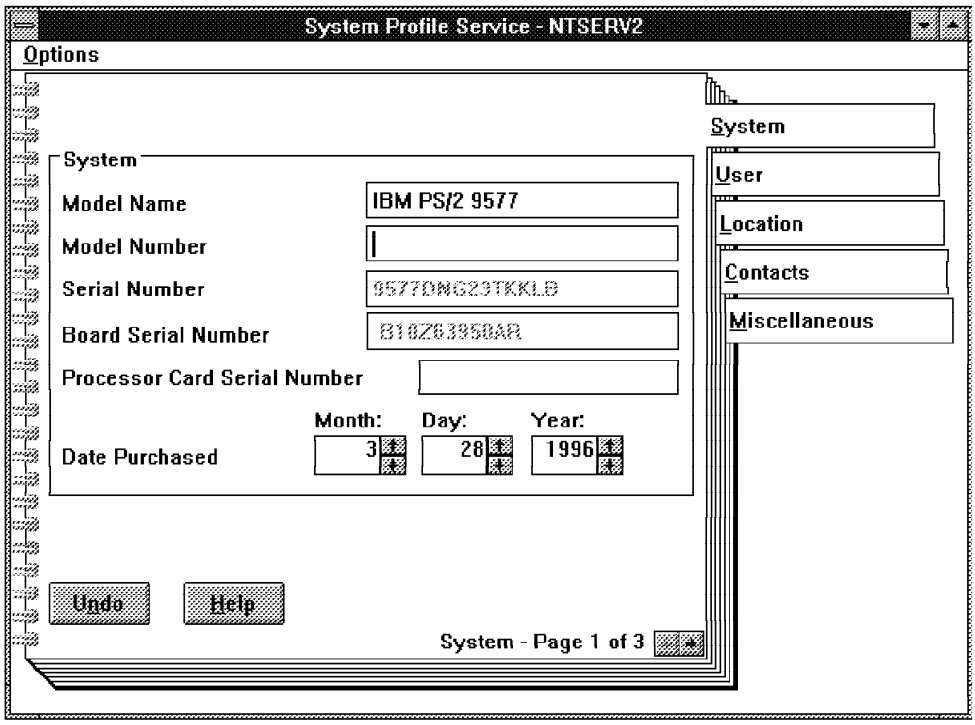


Figure 18. System Profile

In Figure 18 you can see the type of information that could be within the system profile. It automatically inserts information about the system which can be gathered via the System Information service, such as type and model serial number. You may now edit the remaining information. This consists of user information such as name, location, address, telephone number, contact names and also some additional information, which you may define on the so-named miscellaneous pages. These are empty pages, which may be filled with any information depending on your personal needs.

2.1.1.3 Software Inventory

Figure 19. Software Inventory Service

The Software Inventory service is used to collect information about the installed software products on the workstations or servers.

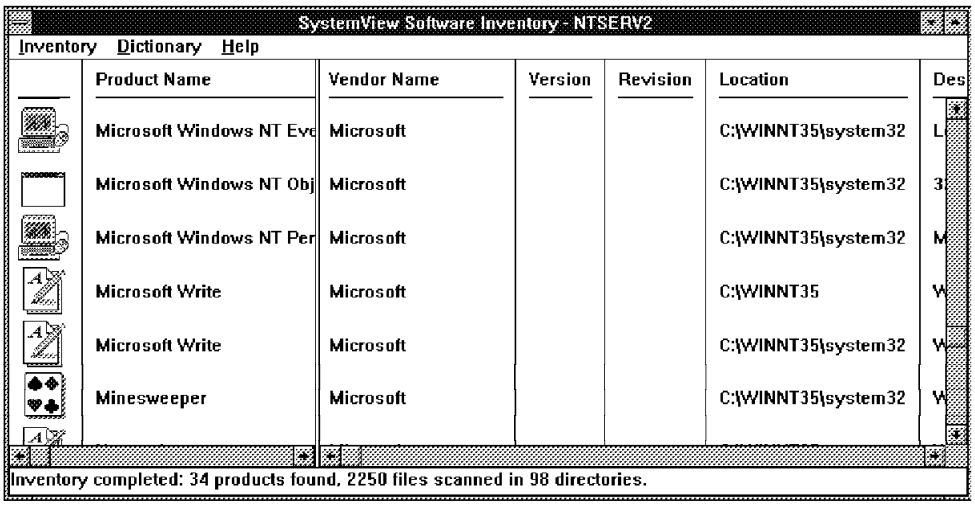


Figure 20. Software Inventory

To obtain information from the Software Inventory service, TME 10 NetFinity uses a built-in database (for example, DEFAULT.SID file), where all the product information can be found for the inventory process. By choosing the **Inventory** pull-down menu you can select different inventory functions such as:

- Full Directory Search

  This function looks for all the products defined within the inventory database (.SID file) and tries to find all products in the workstation. The output lists all the products, which were found including a lot of different additional information such as the location, where the products are installed (see Figure 20).

- Selected Product Search

  When using this function, you will be asked to select one or more of the products from the database, which are being searched for in the workstation.

- Product Type

  You may also only look for a specific type of product. All the software products are divided in product categories such as communication, text and database products.

The display of the product information in this software inventory is identical, independent of the type of search which has been run. In our example in Figure 20 a full directory search has been used. You will get detailed information about the products such as:

- Product name
- Vendor name, which is the name of the manufacturer
- Version and revision level of the product
- Location, which means the drive and subdirectory information where the product is installed
- Description of the product, which is also part of the product database

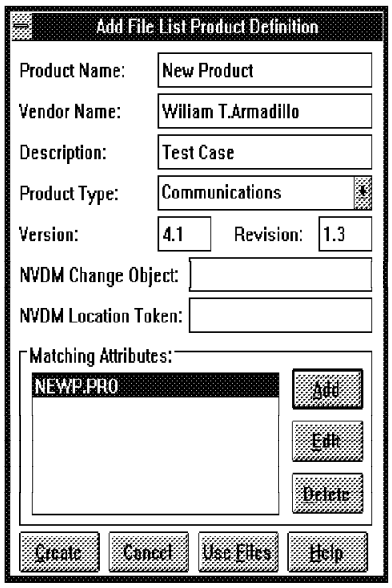


Figure 21. Add New Product

The database (dictionary) for the software inventory can be maintained. You first can select different dictionaries for the inventory search. Then there are more ways to actually update this selected dictionary. You may manually update it by adding, deleting or updating the dictionary information using the dictionary pull-down menu. In Figure 21 you can see an example on how to define or update a new or existing product. Simply select the **Edit** function from the dictionary pull-down menu. Our example shows the different information, that is needed to run later the inventory function. The upper part of the menu is self-explanatory. In the lower part, Matching Attributes, you have to define the file names, for which the inventory function searches to find and identify the product. These can be one or more files. The attributes can also be SYSLEVEL information from OS/2 applications. You also can update it via the import function from the following:

- Software inventory database
- SPaudit dictionary
- QSOFT dictionary
- NetView DM inventory database

2.1.1.4 DMI Services

Figure 22. DMI Icon

The DMI services are used to access the information provided by the DMI layer. DMI (Desktop Management Interface) is a standard interface, which has been defined by many hardware and software manufacturers such as Hewlett Packard, Sun, IBM, Microsoft and Novell. See the separate DMI documentation which is

generally available for details on the DMI interface. You can find information about that at the following Web site:

`http://www.dmtf.org`

All the manufacturers who participated in the DMTF (Desktop Management Task Force) have agreed to implement the DMI standard interface within their products. This interface is used to access management information from the products to manage all the products from different manufacturers with one interface, which means that you can manage different components within your network with only one management product. The DMI interface has not been implemented in every product yet, but you can always see new product announcements from a lot of manufacturers where they have implemented the DMI interface. We can use the DMI browser within TME 10 NetFinity, which is actually the DMI Services, to access this interface. In the following example we show you one of the examples on what kind of information you can get using this function. See Figure 23 for the graphical user interface to access this service.

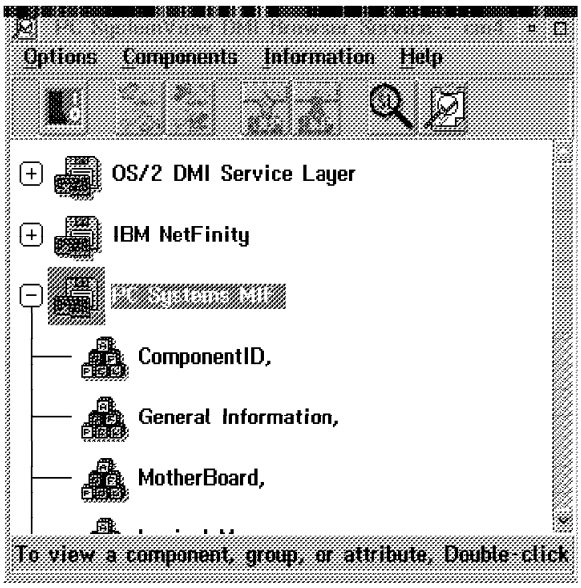


Figure 23. DMI Functions

We accessed the DMI service layer on a remote workstation and received information that the Inventory function did not show. The amount and quality of information from the DMI layer depends on the manufacturer, who implemented the DMI layer in the component. In our case, we accessed the DMI layer of another TME 10 NetFinity workstation. As you can see, you can get a lot of very detailed information about the hardware and software configuration (for example, about hardware adapters and how they are configured). This DMI browsing function can also be used to retrieve information from non-NetFinity components such as hubs and routers. In Figure 24 on page 20 you can see some details of the DMI data flow.

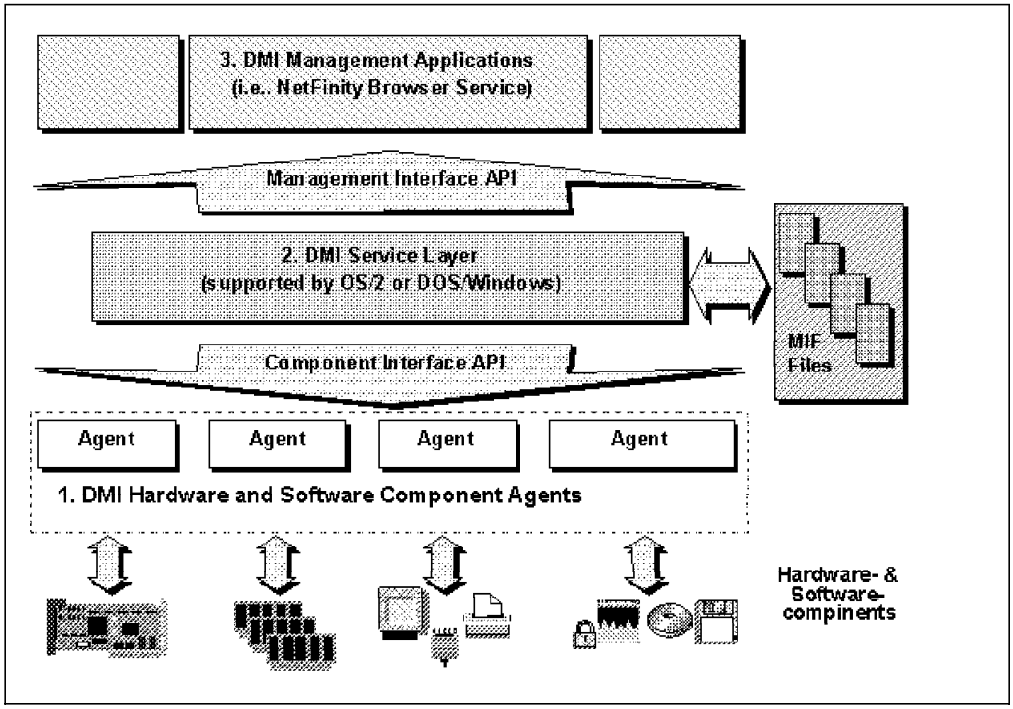


Figure 24. DMI Data Flow

2.1.1.5 Security Manager

Figure 25. Security Manager Service

The Security Manager defines the access profile for accessing the workstation. The definitions will be saved on the workstation and not on the managing workstation. You may define any TME 10 NetFinity Manager user ID and give it different access rights to the different NetFinity Services. This can be done as shown in Figure 26 on page 21.

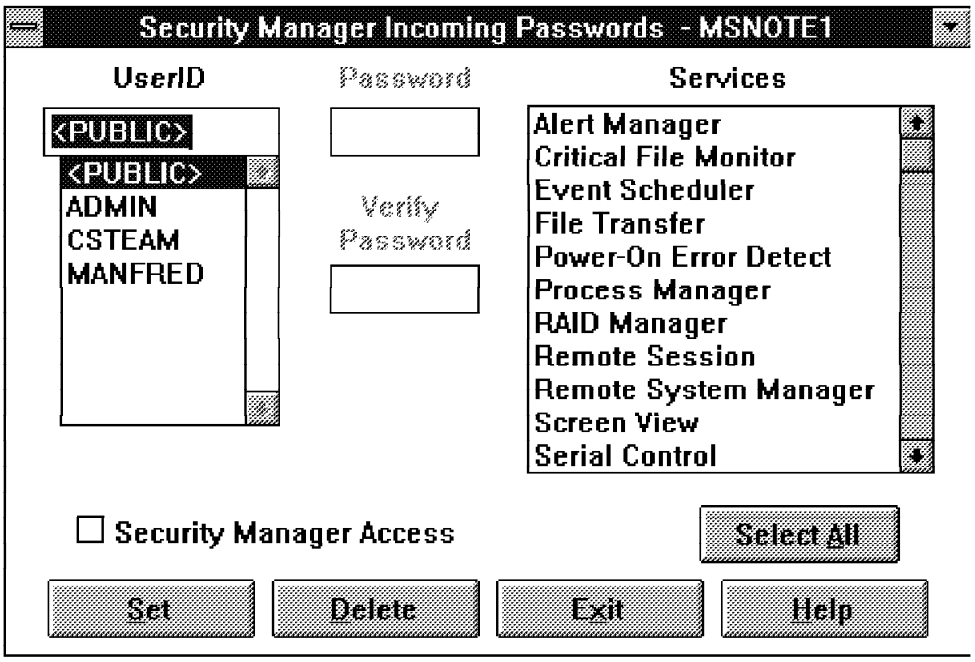


Figure 26. Security Manager

- User ID

  Here you define the different manager users that are allowed to have access to this workstation from a remote manager workstation. Please be aware that the user <PUBLIC> defines the access rights for all users that don't identify themselves with a user ID and password. This means, that in case a NetFinity Manager just hits the Enter key, when asked for a user ID and password without entering it, he or she will be treated as a public user. By default the public users have all access rights to the workstations. Please remember to remove all access rights, after you have defined your first administrator user ID. Please remove the access rights for <PUBLIC> *after* you defined the new users. The new definitions become active right after selecting the Set button. If you make a mistake and delete the PUBLIC user ID before adding another one, the way to reset the IDs back to the default is to delete the SEC.INI file.

- Password/Password Verify

  These are the definition fields where you can define/change the password for the different manager users accessing this workstation.

- Services

  Here you define the different services, to which the NetFinity managers have access. Highlighting a service means access; no highlighting means no access to this service. You can individually select different services for different managers. This is used to restrict the individual access to the different services.

- Security Manager Access

  This the most important definition within this menu. Please be careful with this definition. If a user Security Manager Access has been defined, he or she can create new manager user IDs, passwords and give additional access rights to other users. So this enables managers to define and enhance

complete access rights, even if they have no access rights themselves to one of the other services.

Note: Remember to remove all access rights, including the Security Manager access from the public user. Please define a new manager with Security Manager access, before you remove the rights from the PUBLIC user. If you are doing the security definitions from a remote workstation and you remove the access rights from PUBLIC, you will be thrown out of the NetFinity access to this workstation at the time you choose the Set button. You then no longer have remote access to this workstation, because there has been no manager defined who is allowed to access this workstation.

2.1.1.6 RAID Manager

Figure 27. RAID Manager Service

The RAID Manager service is used to define and control your RAID arrays which are connected to your servers or workstations. It is very important for a network administrator to get all possible information about the disk subsystems especially those that are connected to the network servers. It can be used to do the following:

- Get status information about:
  - RAID adapter
  - Physical drives
  - Virtual drives (arrays)
  - RAID controllers
  - Striping information
- Activate and deactivate drives
- Define and delete hot spare drives
- Create alerts to inform the network administrator about any possible error within the RAID arrays

2.1.1.7 System Partition Access Service

Figure 28. System Partition Service

The System Partition Service can only be used for systems that have a system partition installed. Within a system partition you can find a lot of information about the system configuration. For example, there are ADF (adapter description

files), DGS (diagnostic files) and ADP (adapter description program) files. By changing this information you may also change the system configuration. So be careful who you give access to this service.

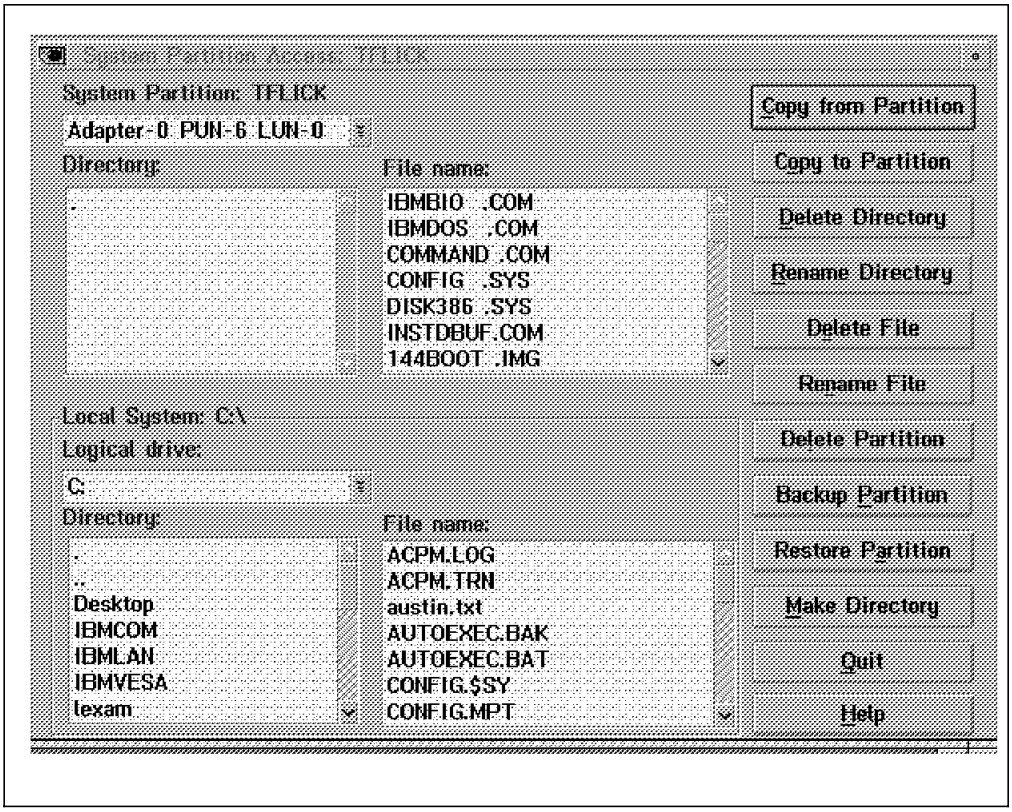


Figure 29. System Partition Access

In Figure 29 you can see how the system partition may be accessed. In the upper half of the menu you can see the contents of the system partition of the remote system named TFLICK. In the bottom half of the menu you can see the drives connected to the local system. You are now able to delete information from the system partition, copy configuration files/drivers from your local drives into the system partition of the remote workstation. See also the additional action buttons for more functions in this menu.

2.1.1.8 Predictive Failure Analysis

Predictive Failure Analysis

Figure 30. PFA Icon

With Predictive Failure Analysis you are able to monitor hard disk drives that are locally installed in your system. You will be automatically notified if one of the PFA drives recognizes an error, which also means that your hard disk drives have to be PFA-enabled. Please check your hardware documentation for the PFA support of your disks.

You may also define an alert due to PFA errors. If a PFA error occurs, you will automatically get an alert depending on how you configured the alert, for example, you may get a pop-up screen. Also see the Alert Manager definitions within this chapter for other types of alerts.

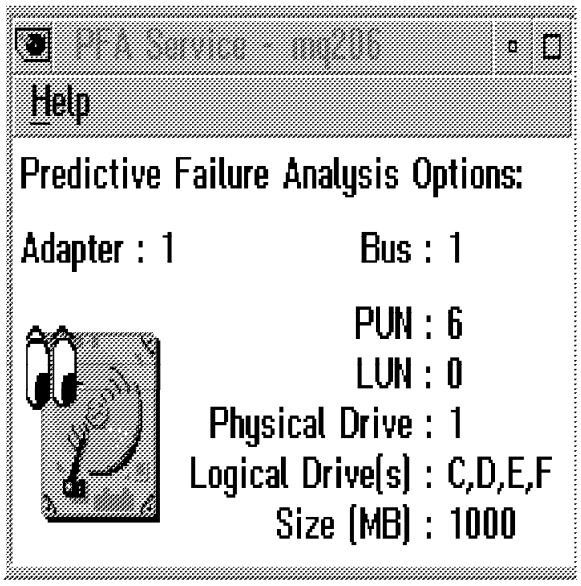


Figure 31. Predictive Failure Analysis

If you display the PFA information via this icon, you may see two different status possibilities.

- Display of hard disk OK, means everything is working fine and no problem was encountered.
- Display of hard disk is shattered, means at least one PFA error occurred. You now have to check the details of this error.

Within the above menu you can get the following information:

- Adapter

  This shows the logical adapter number where this drive is connected.

- PUN and LUN

  This identifies the physical unit and logical unit number, which are assigned to this drive.

- Physical Drive

  The Physical Drive shows the sequence number of this drive starting with 0, 1 or 2.

- Logical Drive

  The drive is actually the logical partition, which has been assigned to this drive such as C or D.

- Size

  The size shows the total space defined for this drive, *not* the remaining space.

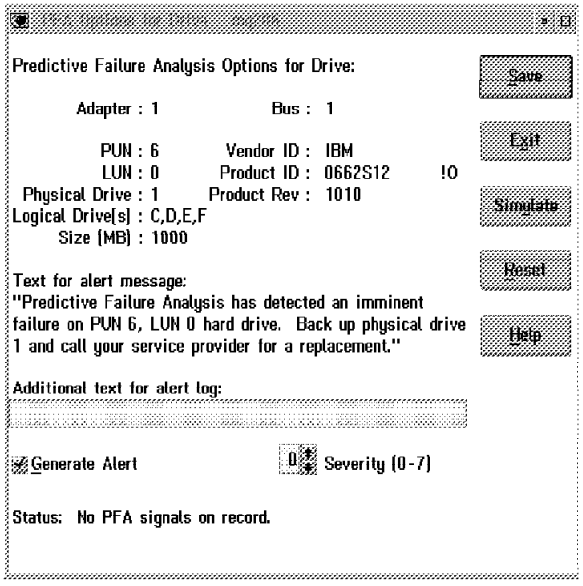


Figure 32. PFA Details

The above menu gives you more detailed information on the errors that occurred on this drive. In addition to the PUN, LUN, you can also see information such as manufacturer and modify the alerts generated by PFA (severity and message text for the alert log).

2.1.1.9 ECC Memory Service

ECC Memory Setup

Figure 33. ECC Memory Service

ECC memory has the capability to correct single-bit errors. A problem might come up that the memory has an increasing amount of memory errors. As long as these errors are just single-bit errors, it is not a real problem because the ECC memory controller takes care of it. But the administrator should be informed about this so that he or she can take appropriate action to have the system serviced before a double-bit error occurs, which will result in a system hang-up. With the ECC Memory Service you can set thresholds to monitor the single-bit errors and create an alert if this value is exceeded. This can be used to take preventive action.

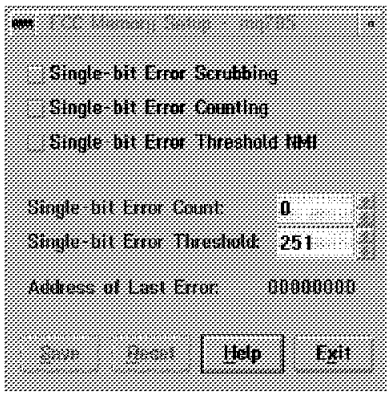
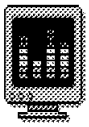


Figure 34. ECC Memory Service Details

2.1.1.10 System Monitor



System Monitor

Figure 35. System Monitor Service

The System Monitor provides a method to monitor the activities of different resources within a system. You can monitor resources such as:

- Locked memory utilization
- Virtual memory utilization
- Disk utilization
- Disk error rate
- Disk space used/remaining
- Processor utilization
- Operating system process and thread counts
- Swapper file information (size and remaining space)
- TCP/IP information such as packets receive/send
- TCP/IP interface details
- LAN server software information such as used sessions and commands

You may also show the information as real-time display or as a line graphics. The information may also be transferred to a database for later use. All monitors can easily be configured to suit your personal needs. If you have a need to monitor a specific component, such as LAN server parameters, which may not be exceeded, then it is possible to define thresholds for all of the monitor functions. These thresholds can then create an alert. The following figure shows some of the examples of the monitors that can be used. There are some differences of the kinds of information you can retrieve from the different NetFinity clients, depending on the operating system on which the NetFinity clients are installed. In Appendix B, “List of Supported Modems” on page 169

you can find an overview of the different information that you may get from the clients. You will find more details on how to use and configure the monitor functions in the *IBM TME 10 NetFinity Services Users Guide*.

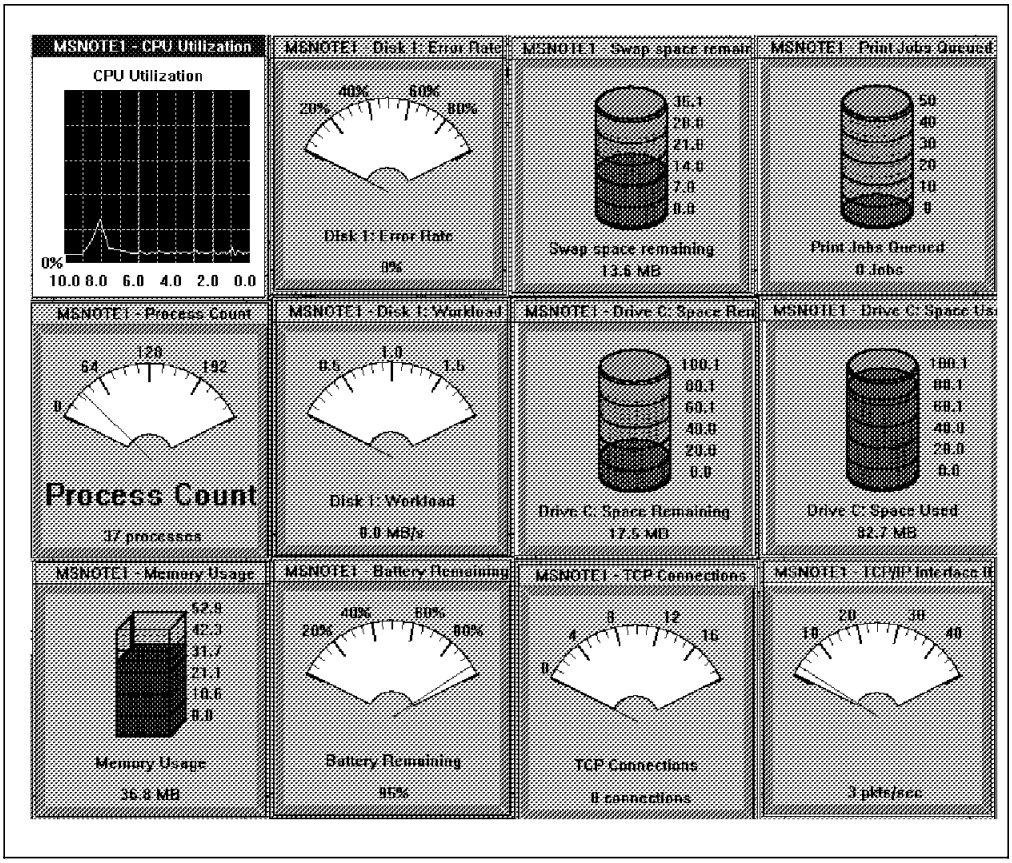


Figure 36. Monitoring

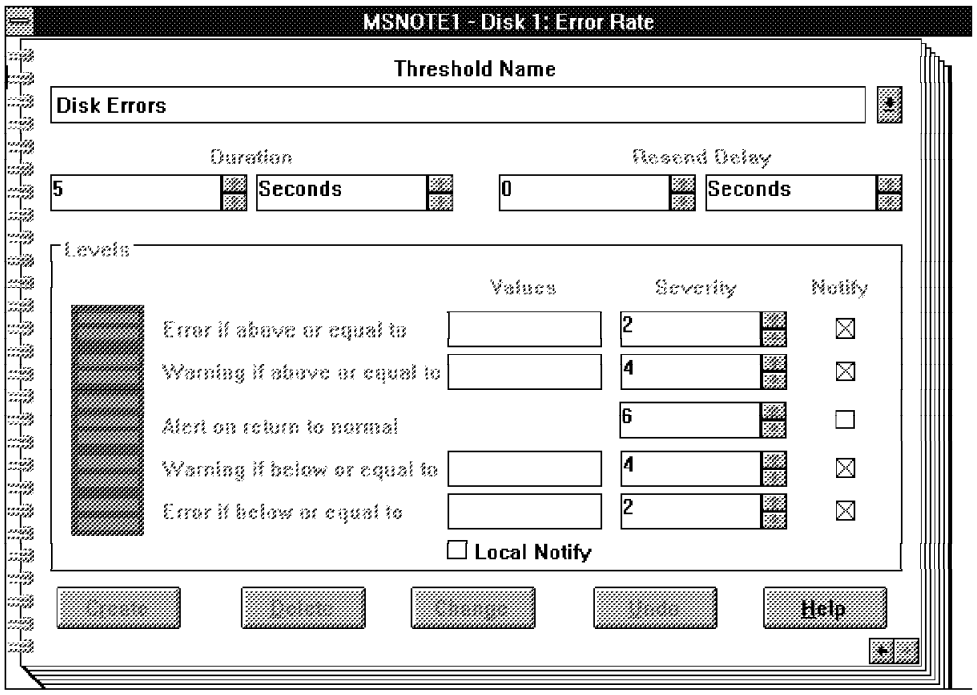


Figure 37. Threshold Definitions

In the above figure you can see how to configure thresholds within the monitor service. You just have to double-click the mouse button on the monitor display to which you want to set up a threshold. Then the threshold definition menu will show up (see Figure 37). You can give this threshold a name and then you have to specify the following data. You first have to define the duration, which means the time, for which the exceeding of the threshold continues before sending an alert. Then specify the resending delay, which is the amount of time the system waits before resending a duplicate alert, because the threshold is still exceeded. Finally, you have to specify the threshold values, which you may put in different categories for the type of alert being issued (error or warning alert) and also if the real value should be lower or higher than the threshold value before sending an alert. 3.2.6, “Applications Sending Alerts to the Alert Manager” on page 104 shows details about the different alerts and how to define and route them.

2.1.1.11 Critical File Monitoring

Figure 38. Critical File Monitor Service

The Critical File Monitor is used to monitor specific files and the access to them; which means that you can define a file within this monitoring function where all access to this file will be recorded by the Alert Manager. The appropriate action defined within the Alert Manager for this alert will be issued. For example, you may define an alert which will then monitor some LAN definition files, which normally nobody, except the LAN administrator is allowed to access. Now, if in this example somebody accesses these LAN definition files, a pop-up window

will be issued with the alert information at the network administrators workstation. See an example on how to configure this in Figure 39 on page 29 and Figure 40 on page 29.

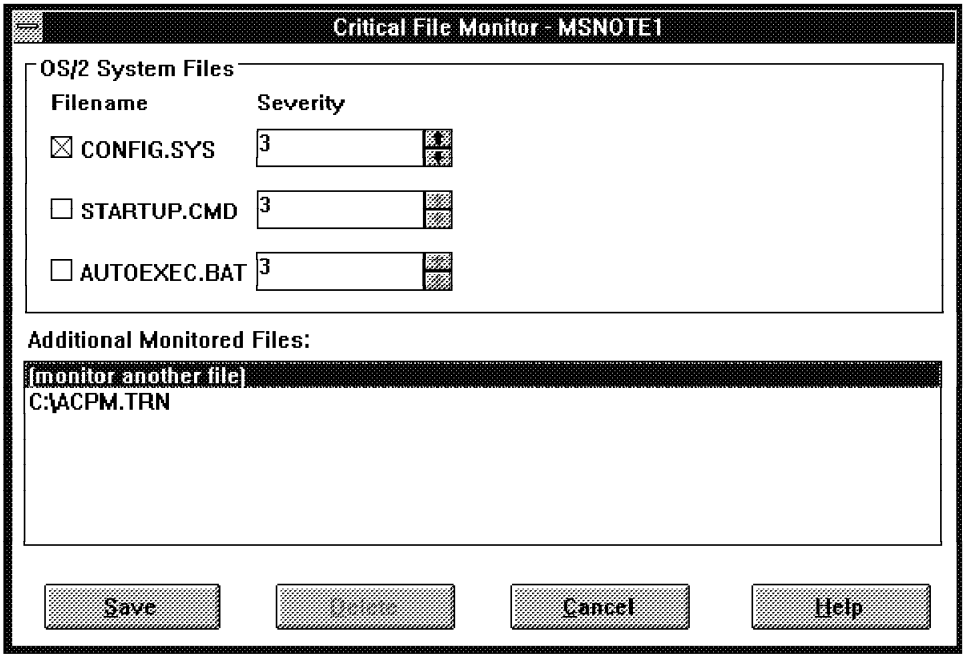


Figure 39. Critical File Monitor

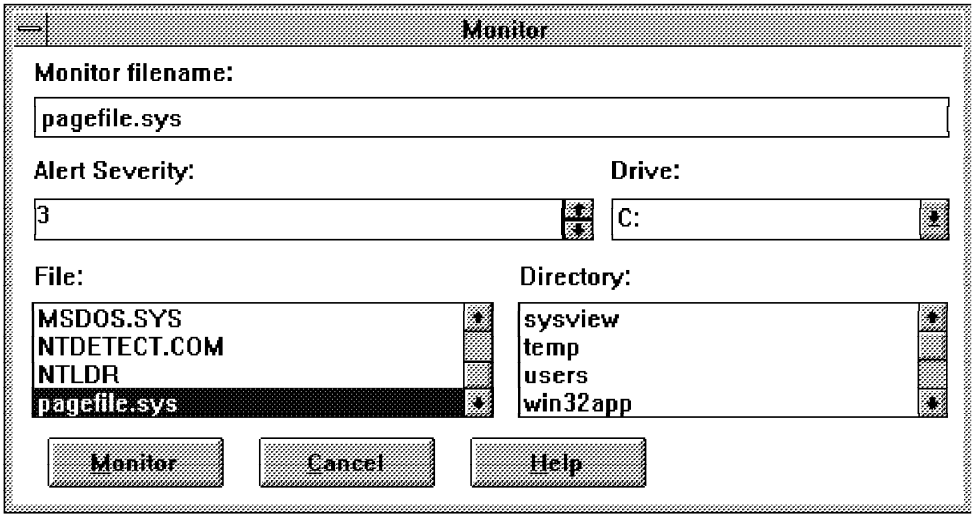


Figure 40. Critical File Monitor Definitions

Within the monitor definitions for the critical files you can define:

- Monitor filename

  This is the name of the file that should be monitored, including the complete path except the drive ID.

- Alert Severity

  The Alert Severity defines the severity for the alert, so that you can separate different alert actions using severity as a criteria from the file monitoring

service. See also the description of the severity subject in 2.1.1.12, “Alert Manager” on page 30.

- Drive

  Here you type in the logical drive ID of your drive where the monitored file is located.

- File and Directory

  These are definition areas that make the definition of the file and path for the file that has to be monitored, easier.

If these definitions have been completed, don’t forget to select the **Monitor** button, otherwise the monitoring has been defined, but is not active.

2.1.1.12 Alert Manager

Figure 41. Alert Manager Service

The Alert Manager enables you to create and react to alerts, which are being created by different originators. A huge variety of actions can be taken due to the occurrence of an alert. These actions are all user-defined. The following are the possible actions that can be defined by the Alert Manager. See also Figure 42 on page 31 for an example of these actions.

- Log an alert in a log file.
- Notify users with a pop-up window.
- Execute a command.
- Forward an alert to FFST/2.
- Forward an SNMP alert.
- Activate a numeric or alphanumeric pager.
- Forward an alert to a specific workstation via a specific protocol.
- Play a waveform.
- Set and remove user-defined error conditions.
- Send out an alert as mail (cc&MAIL or Lotus Notes Mail) to a specified workstation. This requires VIM (Vendor Independent Mail) support.
- Export of an alert to a database. (See the database section of this redbook for details of the different databases.)
- Print an alert.

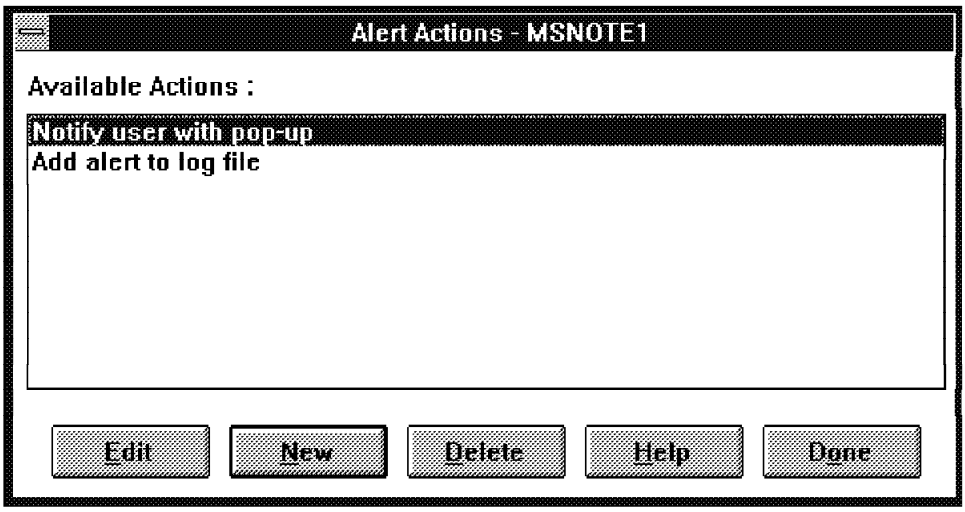


Figure 42. Alert Action List

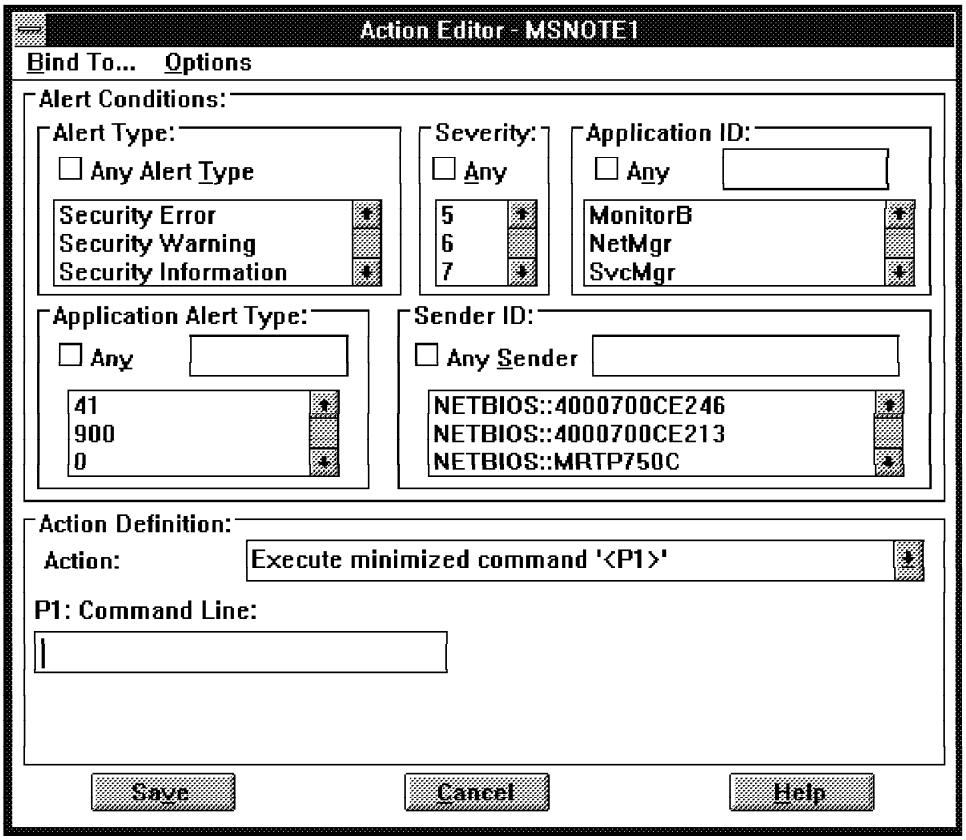


Figure 43. Alert Action Editor

With the Alert action editor, which is accessed by the selecting the **Actions** button of the Alert Log menu shown in Figure 44 on page 33, you can define all the previously described actions due to different error conditions within the system.

- Alert Type

The Alert Type defines what kind of an alert is being issued such as one of the following. You may also define *any* if you want to include all possible alert types.

  - Unknown
  - Information
  - Failure
  - Warning
  - Error
  - All different kinds of alert source information such as system, disk, network, operating system or security

- Severity

  The Severity defines how serious a problem is. Normally you would define severity levels 0-7, where 0 is the most serious condition.

- Application ID

  This application ID is an alphanumeric ID for the different applications that might issue an alert. You can choose one of the given IDs from NetFinity or define your own IDs for your own application.

- Application Alert Type

  The alert type is a numeric value, which is normally issued by an application. To define the proper alert type, have a look at the different application documentation for these types.

- Sender ID

  The sender ID specifies the workstation that may send the alert, including the protocol, as in our example:

```
   NETBIOS::4000700CE246
     |           |
  Protocol     Address
```

  With this definition you can limit the number of received alerts to those alerts, which come from specific workstations. That is, if you are responsible for the TME 10 servers within your network, you may define the protocols and names of the servers you are interested in, so that you only see and possibly react to alerts from these systems.

- Action Definition

  We already discussed the different possible actions at the beginning of this section. Within this field you are going to define the action which is to be taken due to the previous defined alert. You can see the possible actions, which can be defined using the pull-down menu beside this field.

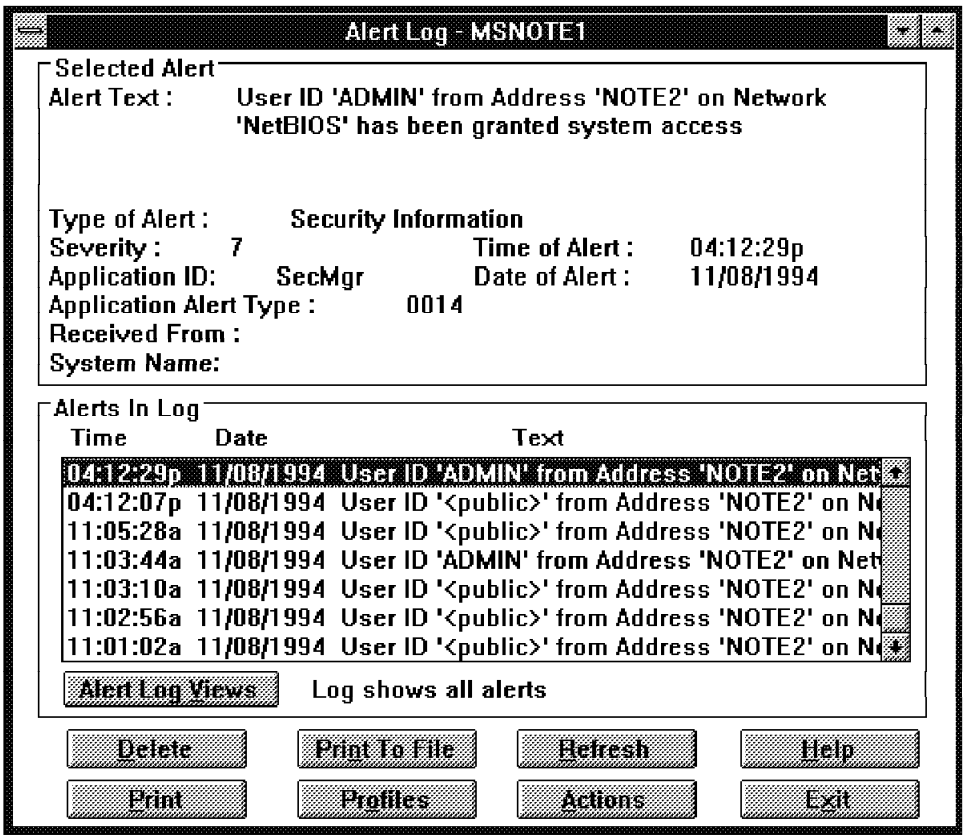

Alert Log - MSNOTE1
Selected Alert
Alert Text : User ID 'ADMIN' from Address 'NOTE2' on Network 'NetBIOS' has been granted system access
Type of Alert : Security Information
Severity : 7
Time of Alert : 04:12:29p
Application ID: SecMgr
Date of Alert : 11/08/1994
Application Alert Type : 0014
Received From :
System Name:
Alerts In Log
Time Date Text
04:12:29p 11/08/1994 User ID 'ADMIN' from Address 'NOTE2' on Net
04:12:07p 11/08/1994 User ID '<public>' from Address 'NOTE2' on N
11:05:28a 11/08/1994 User ID '<public>' from Address 'NOTE2' on N
11:03:44a 11/08/1994 User ID 'ADMIN' from Address 'NOTE2' on Net
11:03:10a 11/08/1994 User ID '<public>' from Address 'NOTE2' on N
11:02:56a 11/08/1994 User ID '<public>' from Address 'NOTE2' on N
11:01:02a 11/08/1994 User ID '<public>' from Address 'NOTE2' on N
Alert Log Views
Log shows all alerts
Delete
Print To File
Refresh
Help
Print
Profiles
Actions
Exit

Figure 44. Alert Log Menu

The Alert Log menu shows you all alerts, which have been issued or received by this workstation. If you select an alert you will see in the upper half of the screen the complete text of the alert. In our case, we selected the first alert issued at 04:12:29 on August 11th. You can see more details about this alert in this menu such as the type of alert, severity, the application which issued the alert and information about the station from where the alert was received. With the action buttons at the bottom of the screen you can start some additional actions. The Alert Log button is used to select the log functions such as restricting the display of the alerts within the different logs. The other buttons are used to control the alert definitions and define and control their output functions. In Appendix A, “Application Alerts and Alert IDs” on page 167 you can find details about the different alerts depending on the application that issued the alerts.

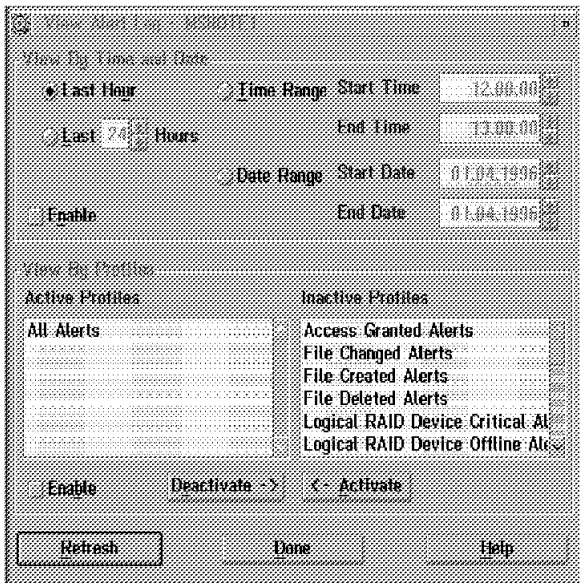


Figure 45. View Alert Log

The Alert Log View is used to modify the way the alerts are shown within the alert log, such as selecting date/time for the display range. You may also select the alert types that you want to look at. You may select different alert types that you want to display from the alert log.

2.1.1.13 Process Manager

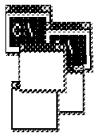


Figure 46. Process Manager Service

The Process Manager service is used to monitor the different processes that are running in a workstation. This monitoring works even if the workstation runs under a different operating system than the manager's workstation.

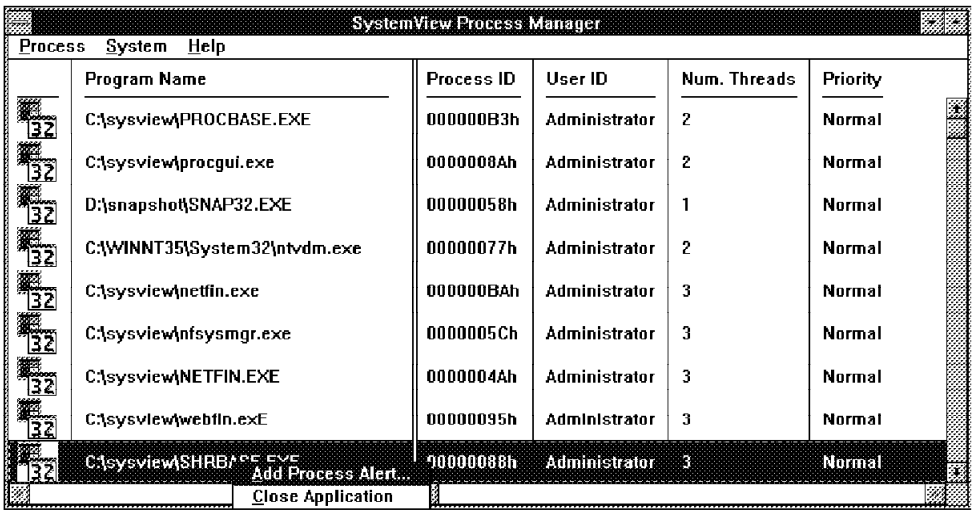


Figure 47. Process Manager Functions

After you select the Process Manager service you receive a complete list of actually running processes. If you now select one of these processes and click the right mouse button, you will get an additional pull-down menu as you can see in Figure 47. The functionality of this pull-down menu depends on the operating system of the remote workstation. You will see the differences of the functionality when managing systems under different operating systems in Chapter 4, “Managing Clients” on page 117. The possibilities if the remote system runs under Windows NT are:

- Add Process Alerts is being used to create alerts from the Process Manager.
- Close Application is used to actually close the running process. This might be useful if you have a hang up situation in your remote workstation, or the user is not able to stop one of the applications.

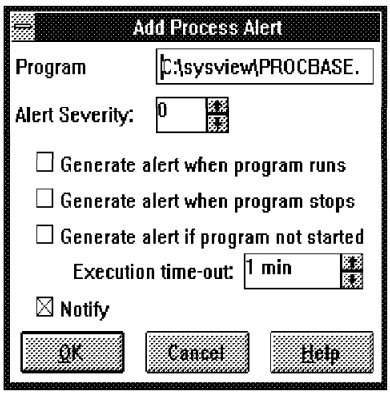


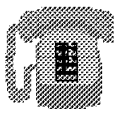
Figure 48. Add Process Alerts

If you want to define a process alert, you can do so by using the above mentioned pull-down menu in the Process Manager service. You will then receive the menu shown in Figure 48, which shows the definitions of this kind of alert. To activate a process alert, you have to provide the information requested in the above menu.

- Program is the definition of the process, which should be monitored, which is actually one of the programs.

- Alert Severity is the severity, which is later being used by the alert manager to identify the alert and issue the appropriate action due to this severity.
- Generate.... depending on the required status of this process you have to select at least one of the conditions, which should lead to an alert generation.

2.1.1.14 Serial Connection



Serial Control

Figure 49. Serial Connection Service

The Serial Connection Service is used to access remote workstations using TME 10 NetFinity and a serial modem link. This service is very useful if you have to support different outlets and you don't have any permanent connection to these LANs or workstations.

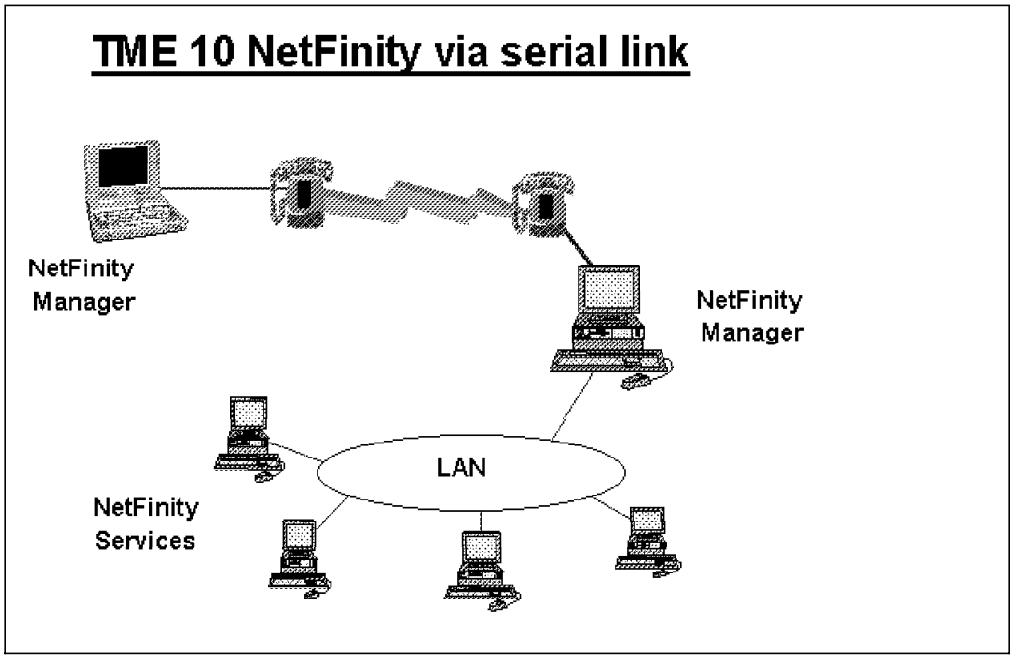


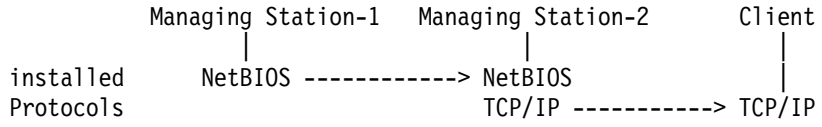
Figure 50. Serial Connection

You can use this service for two the following functions:

1. Connect to a single workstation via a serial link
2. Connect to a remote LAN via a serial link (see Figure 50)

   This means that you are connecting from your manager's workstation via a modem serial link to another managing workstation where the TME 10 NetFinity Manager program is also installed. You are now able to use the Remote System Manager function of the second managing workstation to manage all the workstations connected to this LAN. It is now also possible to do cascading of this managing workstations by connecting one of the TME10s within the remote LAN via a serial link to a third managing workstation and from there manage a second LAN with its workstations.

You may also use this cascading management function to change the communication protocols within the same LAN. This way you can also access a workstation from your managing station, even if the client only has a network protocol driver installed, which you don't have on your workstation. In our example the network administrator is working at the local Managing Station-1, which only has the NetBIOS protocol driver installed. He or she now accesses Managing Station-2, which has the NetBIOS and TCP/IP protocol drivers installed and active. Then the network administrator uses the Remote System Manager function of that Managing Station-2 to access the client via the TCP/IP protocol. Please see the example below for details:



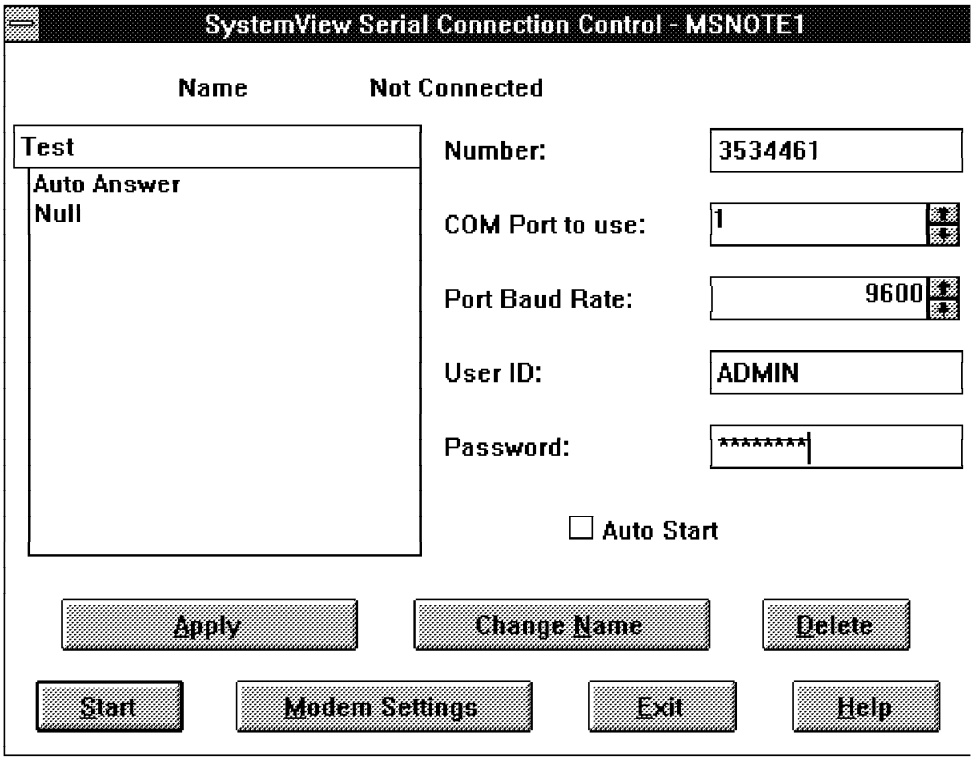


Figure 51. Serial Connection Control

The connection control is used to define all possible connection using the serial link support of TME 10 NetFinity. In general we have two possibilities:

1. Running as a client, then defining a modem connection with Auto Answer.
2. Running as an active NetFinity Manager, then defining a modem connection with a unique name.

- Name

  The name is used to identify the connection. Please specify a name that might be logical to this connection, such as defining the name CHICAGO for the connection to your outlet in Chicago.

- Number

  Phone number, which is used to dial to the remote workstation.

- COM Port to use

  Select the appropriate COM port, where the modem is connected to.

- Port Baud Rate

  Select the baud rate for the data transfer to the remote workstation.

- User ID

  The user ID is used to identify your managing workstation to the remote workstation. See also the Security Services definitions in your remote workstation for the appropriate user ID.

- Password

  This is the password for the above mentioned user ID.

- Auto Start

  The Auto Start function is used to automatically connect to a remote workstation during startup time of TME 10 NetFinity or to automatically activate the auto answer feature, so that requests from a managing station can automatically be received and answered.

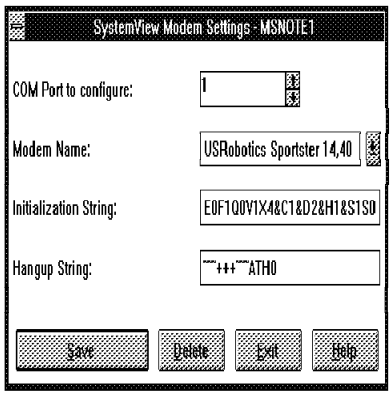


Figure 52. Modem Definition

Within the modem definition function, which you may have selected in the previous menu, you define your modem settings such as modem type/model, initialization strings and COM ports. See Appendix B, “List of Supported Modems” on page 169 of this book for a list of preconfigured modems. Of course you can change any of the modem definitions to fit your needs and you may also add additional modem definitions. These preconfigured modems are stored in the file SERMODEM.DAT in the NetFinity subdirectory, but you should not manually change the definition within that file. Make all required changes via the graphical user interface of TME 10 NetFinity.

2.1.2 TME 10 NetFinity Functions for Manager

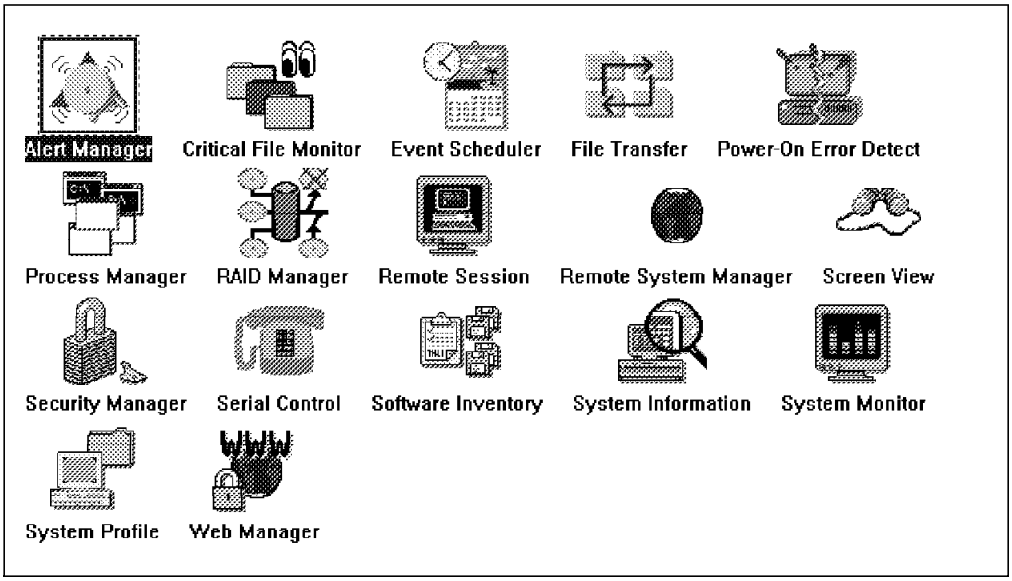


Figure 53. Remote Administrator Service

The user interface shown in Figure 53 shows all the available functions that can be used for the workstation which you have accessed, which means, that only those functions that are supported by the remote workstation are shown within the menu. In addition the supported functions at a workstation can still be limited by the Security Manager function, which will be explained later within this chapter. If a function is not allowed to be used by the manager, who is identified with the user ID, then this function will not be shown for this manager, even the system supports this function.

2.1.2.1 Remote System Manager

Remote System Manager

Figure 54. Remote System Manager Service

The Remote System Manager is used to access remote workstations. To easily access these stations to have to define them in groups as shown in Figure 55 on page 40. You can name the groups as you like, but for practical reasons you should give them logical names. You are able to define them in different ways:

- Define a group with no keywords. You will see via the discover function, which actually does a broadcast, that all TME 10 NetFinity workstations will show up. This might be too confusing.
- You may also define groups with an and/or combination possibility by using the keywords that have been defined during the installation process. The keywords do not have to be unique. It might be an idea to use for example, the keyword SERVER for all TME 10 server systems in the network. So if you use the word SERVER as a keyword for this group, then automatically all server systems will show up within this group.

- You may also limit the workstation within a group not only by using keywords, but also by using Discovery Filters, which can be defined by clicking on the right mouse button on a group, then selecting **Discovery Filters**. You may now limit the workstations in this group by selecting the operating systems such as Windows 95, OS/2 and NetWare. Also you can select the protocols that are being used to access protocols such as NetBIOS, IPX and TCP/IP.

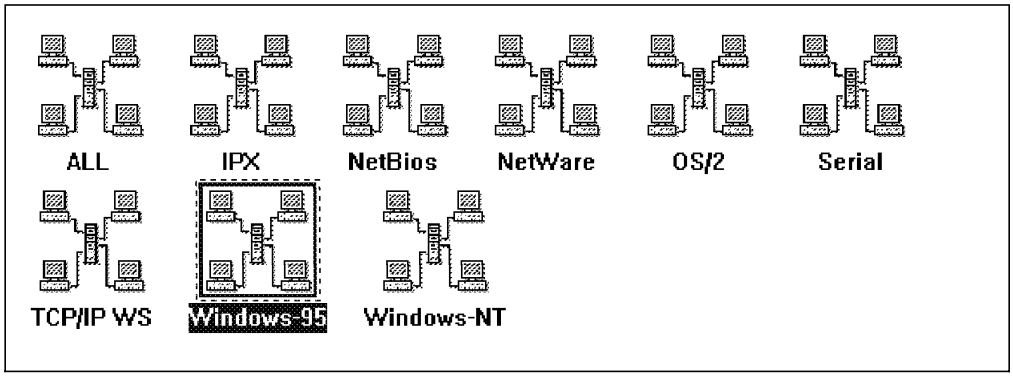


Figure 55. Group Management

If you now select one of the groups that you already defined, you can have two different ways to display the workstations. First you should do a discover via the System pull-down menu. Now all systems that belong to this group will show up. If one of the systems has been discovered once within this group, then it stays in this menu, even if becomes offline for any reason. You can easily recognize an offline system by its icon color. If a system has got a problem, but did not go offline, you will see a special error sign at these icons. In Figure 56 on page 41 and Figure 57 on page 41 you will see a group display. The difference between these displays is that the figure titled Group View - Icons was defined with Icon View via the View pull-down menu and the figure titled Group View - Details was defined with Detail View.

With the Icon View you can just see all systems belonging to this group as an icon. You get the system name information if this system is a TME 10 NetFinity manager or services and if this system runs as a LAN server independent if it is Windows NT Advanced Server, OS/2 LAN Server or NetWare.

With the Detailed View you get more detailed information in addition to the information given by the Icon View.

- Network protocol, which is used for this connection. If there has been more than one protocol driver configured for TME 10 NetFinity, than this system appears more than once in this table (in our example the workstation named SVCLI1). This workstation has NetBIOS and TCP/IP protocol enabled.
- Network address, which is protocol-dependent information, such as the NetBIOS name for the NetBIOS workstations.
- System and model description, if the system type can be identified by TME 10 NetFinity.
- Also the type and version of the installed operating system will be shown in this table.

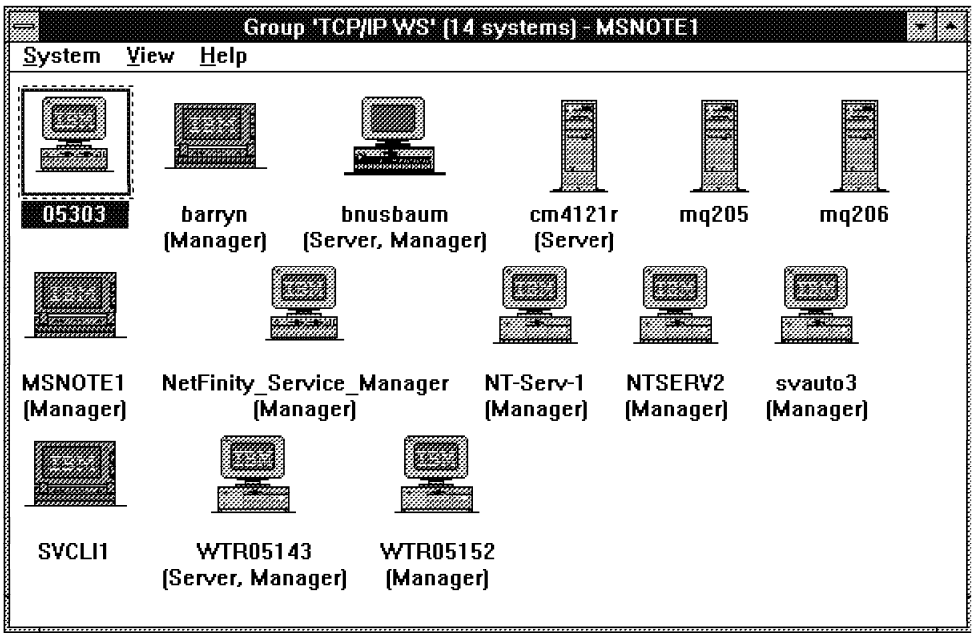


Figure 56. Group View - Icons

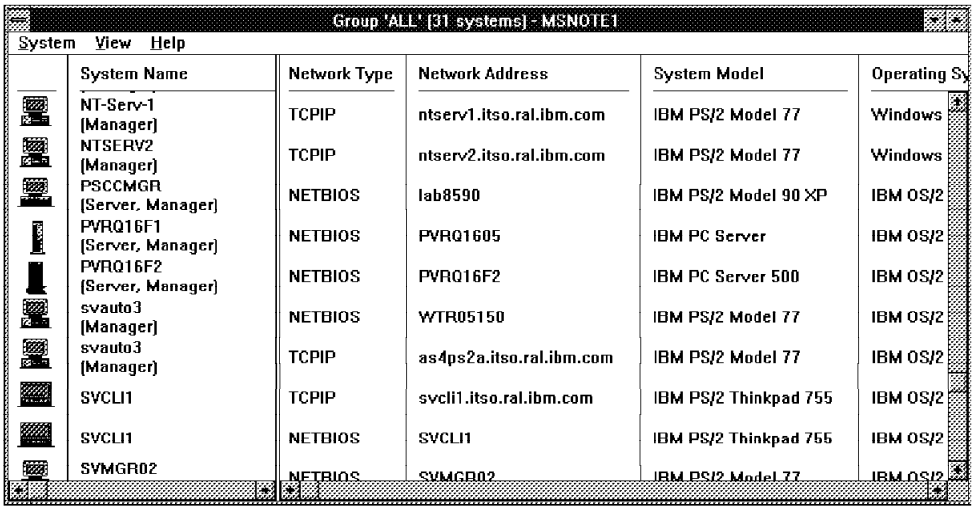

Group 'ALL' [31 systems) - MSNOTE1
System View Help
System Name
Network Type
Network Address
System Model
Operating Sy
NT-Serv-1 (Manager) TCPIP ntserv1.itso.ral.ibm.com IBM PS/2 Model 77 Windows
NTSERV2 (Manager) TCPIP ntserv2.itso.ral.ibm.com IBM PS/2 Model 77 Windows
PSCCMGR (Server, Manager) NETBIOS lab8590 IBM PS/2 Model 90 XP IBM OS/2
PVRQ16F1 (Server, Manager) NETBIOS PVRQ1605 IBM PC Server IBM OS/2
PVRQ16F2 (Server, Manager) NETBIOS PVRQ16F2 IBM PC Server 500 IBM OS/2
svauto3 (Manager) NETBIOS WTR05150 IBM PS/2 Model 77 IBM OS/2
svauto3 (Manager) TCPIP as4ps2a.itso.ral.ibm.com IBM PS/2 Model 77 IBM OS/2
SVCLI1 TCPIP svcli1.itso.ral.ibm.com IBM PS/2 Thinkpad 755 IBM OS/2
SVCLI1 NETBIOS SVCLI1 IBM PS/2 Thinkpad 755 IBM OS/2
SVMGR02

Figure 57. Group View - Details

If you now select one of the workstations shown within this group and the public access to this workstation has been removed, you will receive a pop-up window for entering a user ID and a password to access the station. After entering the requested information, you will receive a menu with all the authorized TME 10 NetFinity services for this particular user ID, which you used to log on.

2.1.2.2 Event Scheduler

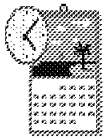


Figure 58. Event Scheduler Service

Up until now, we only discussed the different services that can be used manually by a TME 10 NetFinity manager. The Event Scheduler service can be used to run several services automatically time and date controlled.

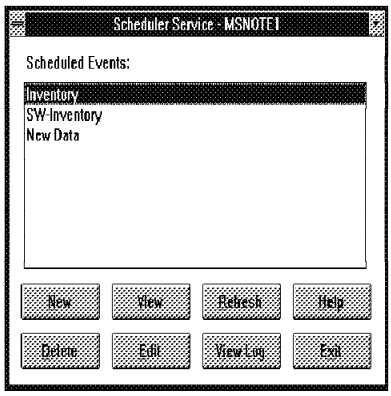


Figure 59. Event Scheduler - Event List

After you select the Event Scheduler service, you get a list of events that have already been defined. You may add, delete or modify any of these events. Let's define a new event for this service.

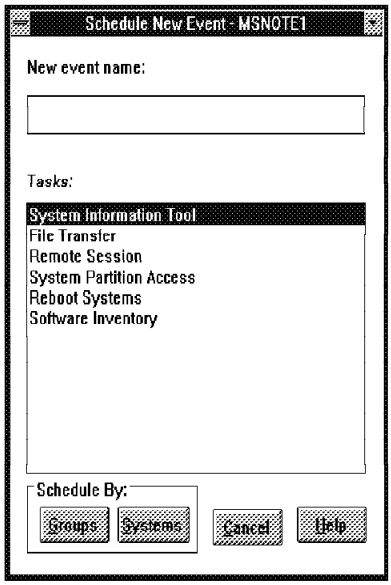


Figure 60. New Event

First you have to define an event name, which will later be shown in the above mentioned event list. Then select one of the available TME 10 NetFinity services, which might be limited by your manager's user ID. Then you have to select the task, which is one of the available services. You now have to select the way of selecting the workstations that you want to access by selecting the action buttons Groups or Systems. With the Group selection you only have a chance to define a complete group of workstations, but you cannot exclude or include a workstation to this list. With the System selection you can select groups of workstations and also include single or multiple additional workstations. See Figure 61 for a selection by groups. We selected the group Windows-NT, which in our example consists of all workstations that have the Windows NT operating system installed.

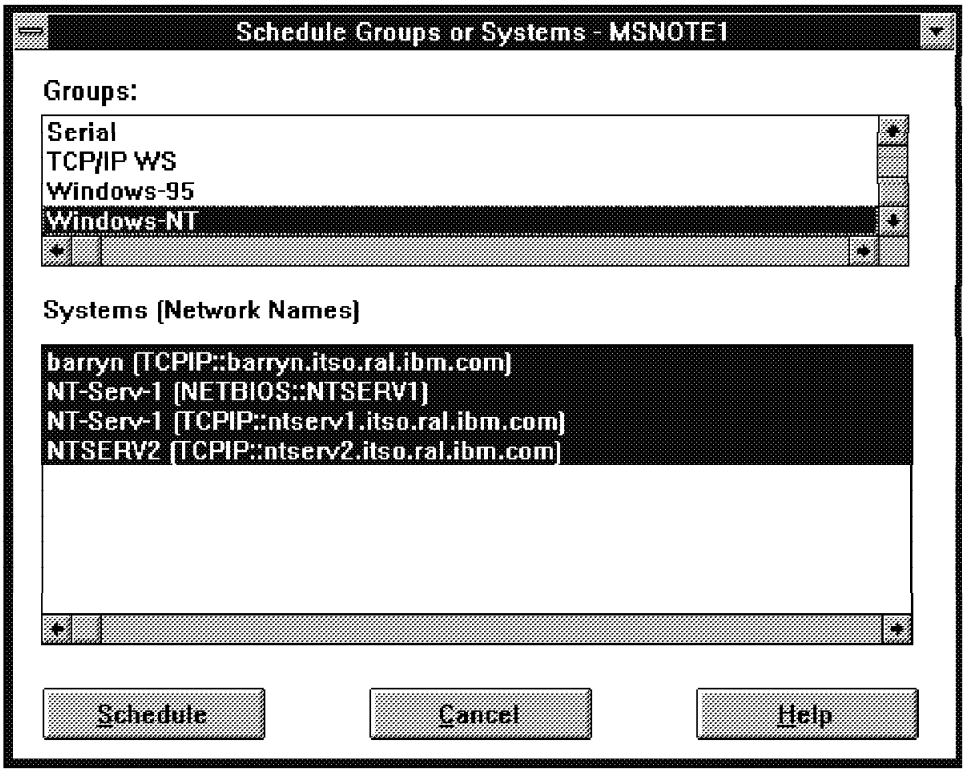


Figure 61. Events Group Selection

You now have to select the **Schedule** button to define where the output has to be sent. You can define a history file or an ASCII file. This ASCII file may also be sent to a printer instead. If you select that the output should be sent to a database, then more database definitions have to be done. See also the database section of this book for definitions.

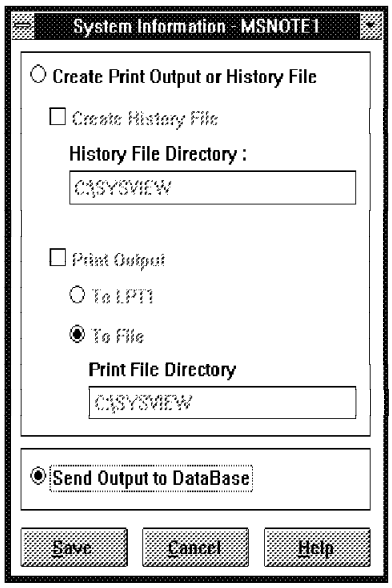


Figure 62. Output Definitions

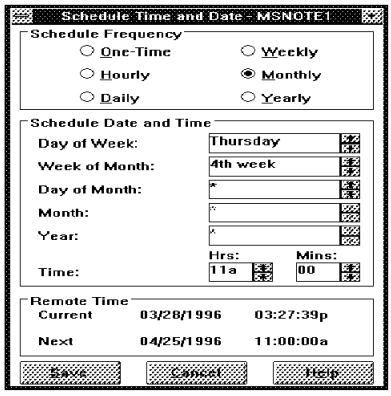


Figure 63. Schedule Time and Date

In the menu shown in Figure 63, you now define the frequency and the time schedule for this event. You may define a one-time event as well as repeating events (daily, weekly, monthly and yearly). Depending on your selection you also have to give now more details about time and date. After you finish the definitions, click on the **Save** button to save the configuration and the newly defined event becomes automatically active. In our example we used the System Information Service. This might be used to create an inventory database.

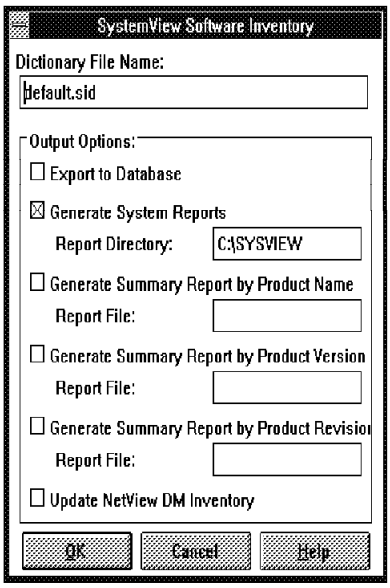


Figure 64. Schedule SW Inventory

You can also use other functions such as Software Inventory or File Transfer service. You always have to define the event name, service and frequency. Depending on the defined service you may have to give more details. See Figure 64 for a software inventory example. With software inventory you can create outputs that do the following:

- Export to a database.
- Generate system reports that show a complete software inventory sorted by systems.
- Generate summary reports by product name, which gives you a file that includes all installed software sorted by the name of the product. This means that you only get information about each product such as product name, manufacturer, version and number of licenses installed.
- Generate summary reports by product version, which gives you a file that includes all installed software sorted by the version of the product, which means, that you only get information about each product such as product name, manufacturer, version and number of licenses installed.
- Generate summary reports by product revision, which is the same report as mentioned above only it is sorted by the revision level of the products.
- Update NetView DM inventory database (self-explanatory).

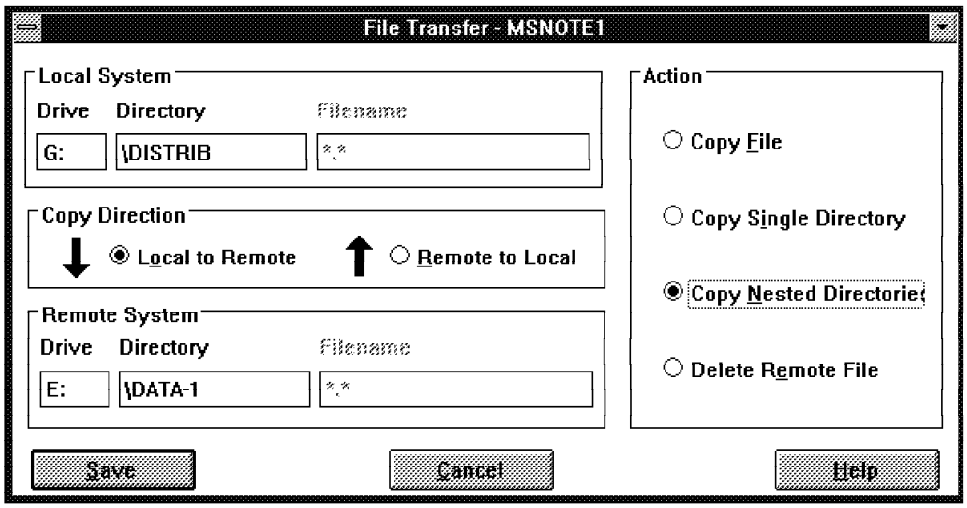


Figure 65. Schedule File Transfer

The File Transfer Service in the event scheduler enables you to transfer data to multiple systems at the same time. You then can define the source and target information and define, if you want to copy a single file, single directories or nested directories. In addition, you may also delete files and directories on remote workstations.

2.1.2.3 File Transfer

File Transfer

Figure 66. File Transfer Service

The File Transfer service is used to copy data from and to a workstation without any LAN server/requester software being installed. Also for this service you only need TME 10 NetFinity and one of the supported network device drivers installed.

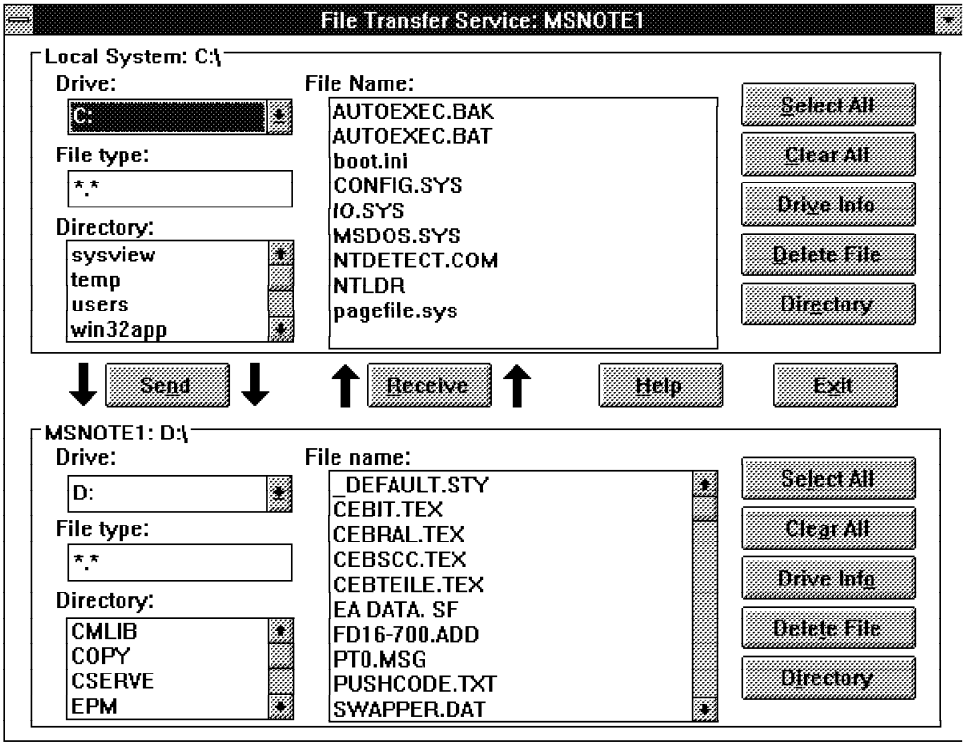


Figure 67. File Transfer Menu

In the upper half of the File Transfer menu (see Figure 67) you can see the local devices, which are installed in your managers workstation or are logically connected to it using a LAN requester software. In the lower half of the window you can see the drives, which are located in the remote workstation or connected to it by using LAN resources defined by a LAN server software. You can see the logical name of the remote workstation at the top of the lower half of the menu. In our example its name is MSNOTE1.

You can now transfer any files from and to the remote workstation by selecting a single file as well as a set of files and complete subdirectories contents and their nested directories. These files don't have to be copied to the same subdirectory name on the target system. You can select any drive and subdirectory. The File Transfer service compresses and decompresses the files for the transfer to speed up this process. This transfer process is just for a copy of files to a single workstation. If you want to do a copy from or to a group of workstations, then you can do this by using the Event Scheduler Service of TME 10 NetFinity, which has already been described earlier in this chapter.

2.1.2.4 Power-On Error Detect

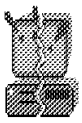


Figure 68. Power-On Error Detect Service

The Power-On Error Detect (POED) Utility listens to the network segment for systems sending error alerts during the power-on self test. Only systems with a

system partition can use this function. See 3.1.1, “Alert Manager” on page 95 for a description on how to define a workstation, so that it is enabled to send POED alerts. It will send a broadcast package to all systems running the POED Service. If you have a central systems manager to control all workstations in a multiple segment network, you need at least one system running the POED service per segment and forward the alert to the central manager.

Without the POED service on the workstations, the error recovery during the POST phase runs in the following way:

1. The system detects an error during the POST test.
2. The error code is being displayed on the screen.
3. The system goes to the system partition and loads a test routine.

Now with POED activated in the workstation, it works similar, except that after going to the system partition, it loads a previously defined network device driver and sends out a broadcast alert with the error information.

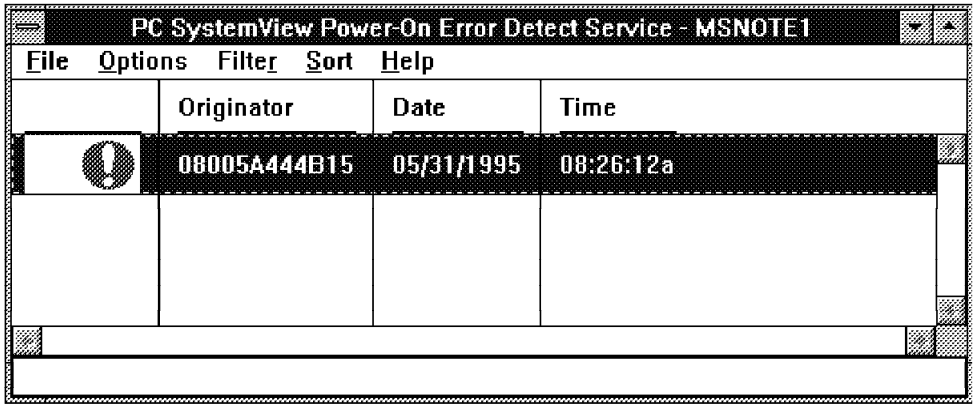


Figure 69. Power-On Error Detect

After the workstations have been defined to send out the error alerts and your manager has been defined to receive these errors, you are now able to have a look at the errors that may have happened during POST. See the above figure for such an alert. In this entry you can see the following details:

- Originator, which is the adapter address of the sending workstation
- Date/Time, which are the appropriate date and time of the error

If you now click on the entry, you get more details (see Figure 70 on page 49).

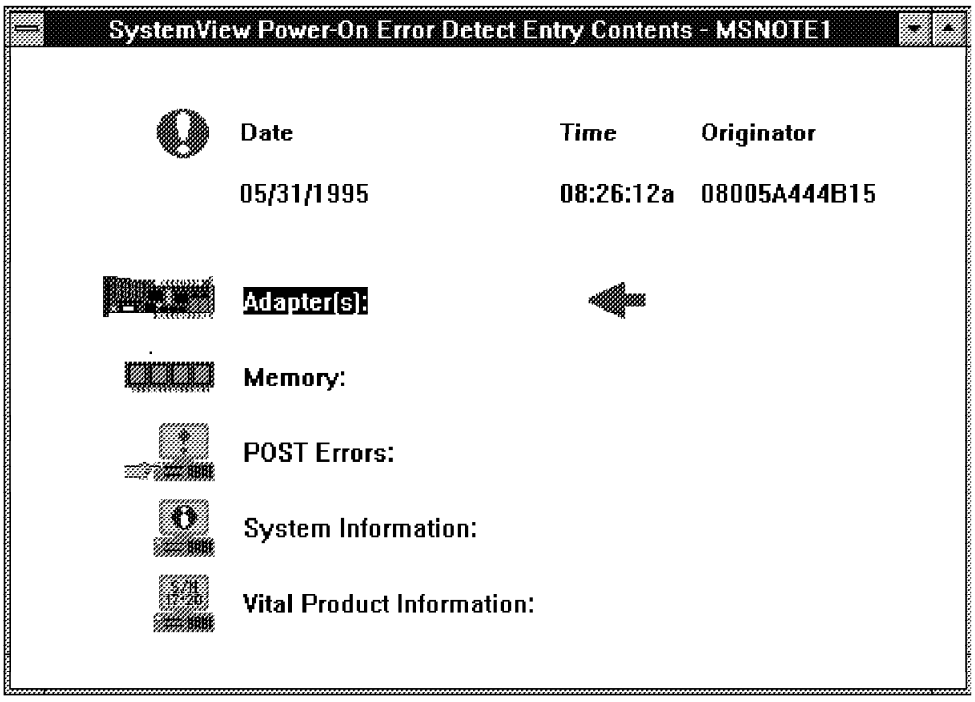


Figure 70. POED Entry

Within the menu shown above you can see some more details about the POED error. The arrow shows the component that issued the error condition. In our case it says that there is an error within the adapter configuration. If you click on the Adapter icon, you will receive the window shown in Figure 71.

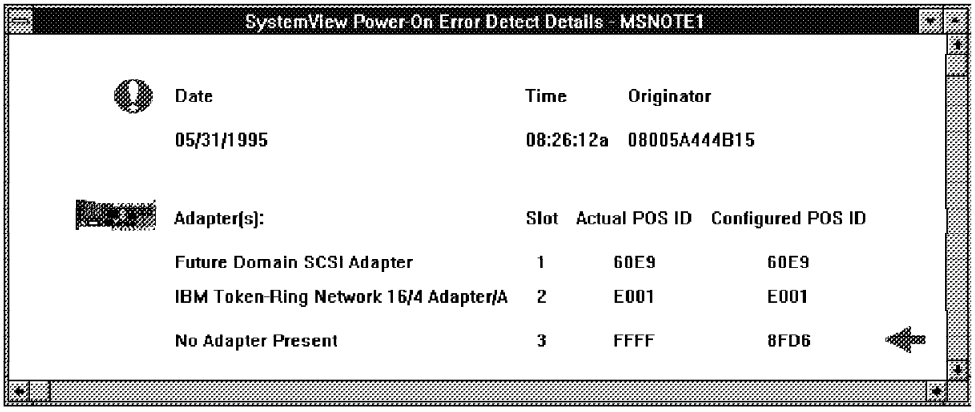


Figure 71. POED Entry Details

Within this menu we can see that the error came from adapter slot 3, which shows that the adapter was not responding during power-on. The configured adapter has an ID of 8FD6. This can be used to identify the type of adapter that is missing. This error may have happened, because the adapter is not functioning properly or is missing. In our case, we simulated this error and removed the adapter in slot 3 before we powered off this workstation and then on again. You can see that we can get a lot of very detailed error information from a workstation, even if the operating system is not running at the time of the failure. But remember, that you need to have workstations that have a system partition installed to create this kind of alerts.

2.1.2.5 Remote Session

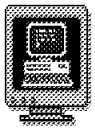


Figure 72. Remote Session Service

The Remote Session Service can be used to start and control a command session that runs in the remote workstations. This means, for example, if the remote workstation is a Windows NT workstations, then a DOS command prompt will be started in the background of the remote workstation. This session will be controlled by the manager.

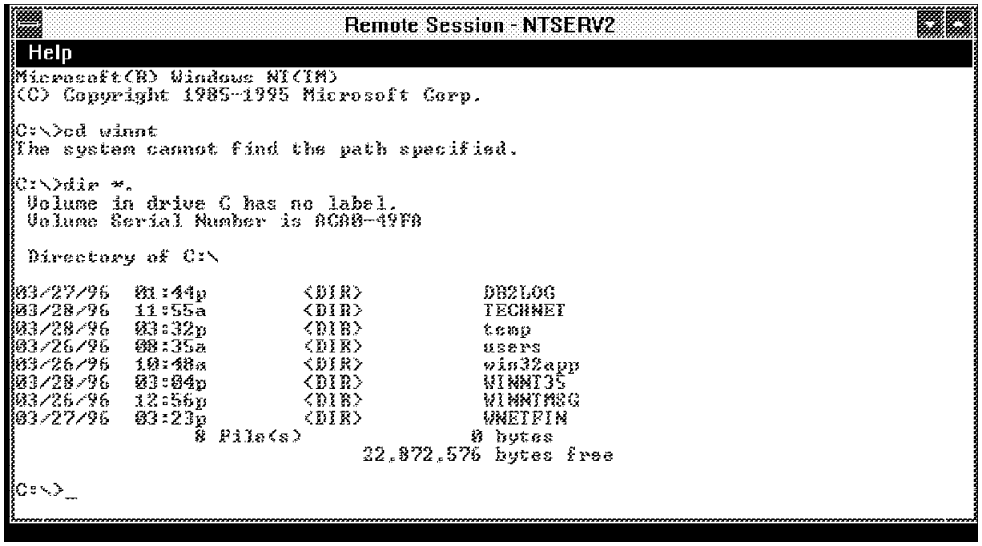


Figure 73. Remote Command Session

The manager sees the window shown in Figure 73, which is the contents of the command session in the remote workstation. You are now able to issue DOS or for an OS/2 workstation, OS/2 commands. Whatever is done in this session, (for example, typing a command) is first sent to the command session in the remote system and then will be displayed in the Remote Command Session window of the managers workstation. The user at the workstation can see, what is done in this session if he or she switches to it using the task selection of his or her operating system. Both the user at the remote workstation and the manager can now work in this session and for example enter commands. Whoever types first, their data will be entered first. This might also be useful for some help desk functions.

2.1.2.6 Screen View

Screen View

Figure 74. Screen View Service

The Screen View service is an easy way to capture a screen from the remote workstation. This screen contents is saved and sent to the managing workstation as a bit map file. The screen contents therefore may also be saved in a file at the managing workstation for later problem determination and problem tracking. Also, in case of an error at a workstation, very often there are communication problems between the user and the help desk staff. It is very complicated to communicate the error information from a screen via the phone. So this is a useful tool to get information about an error condition at a workstation and also save the screen contents to a file, which is also possible via this function.

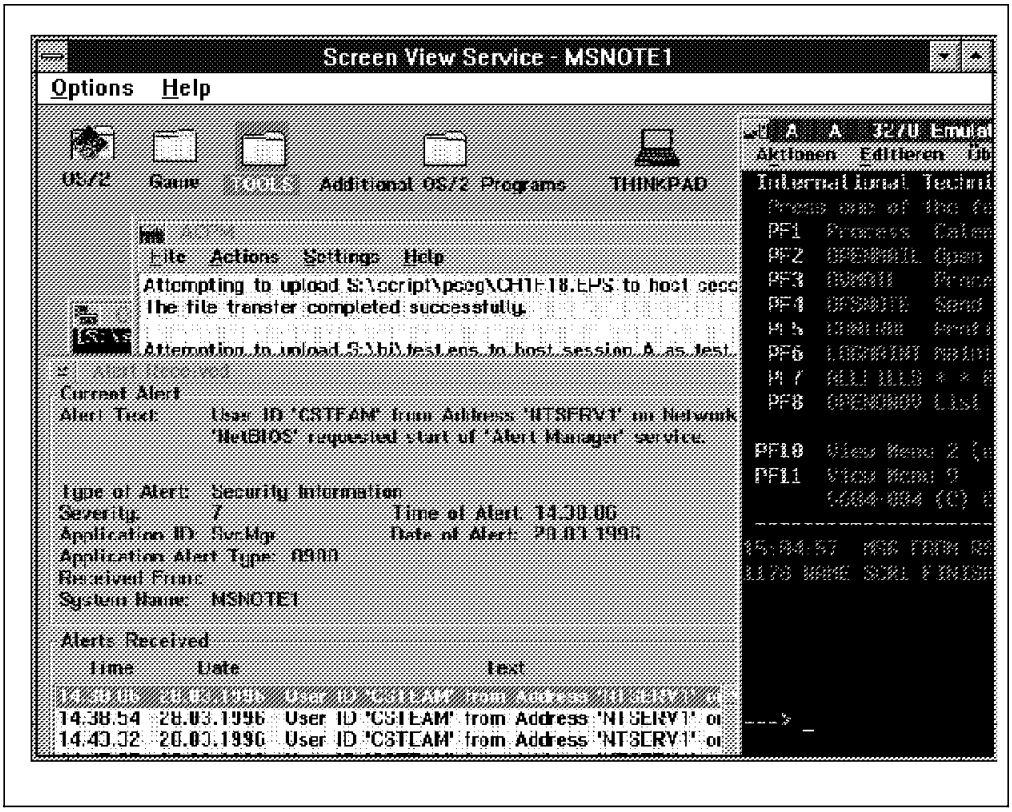


Figure 75. Screen Capture

There is no way to work on the graphical user interface, which is captured with the Screen View service. This only gets information from a workstation.

2.1.2.7 Web Manager

Figure 76. Web Manager Service

The Manager Service is used to connect to remote workstations over the Internet or an intranet. Figure 77 shows the connection to remote LANs using this facility.

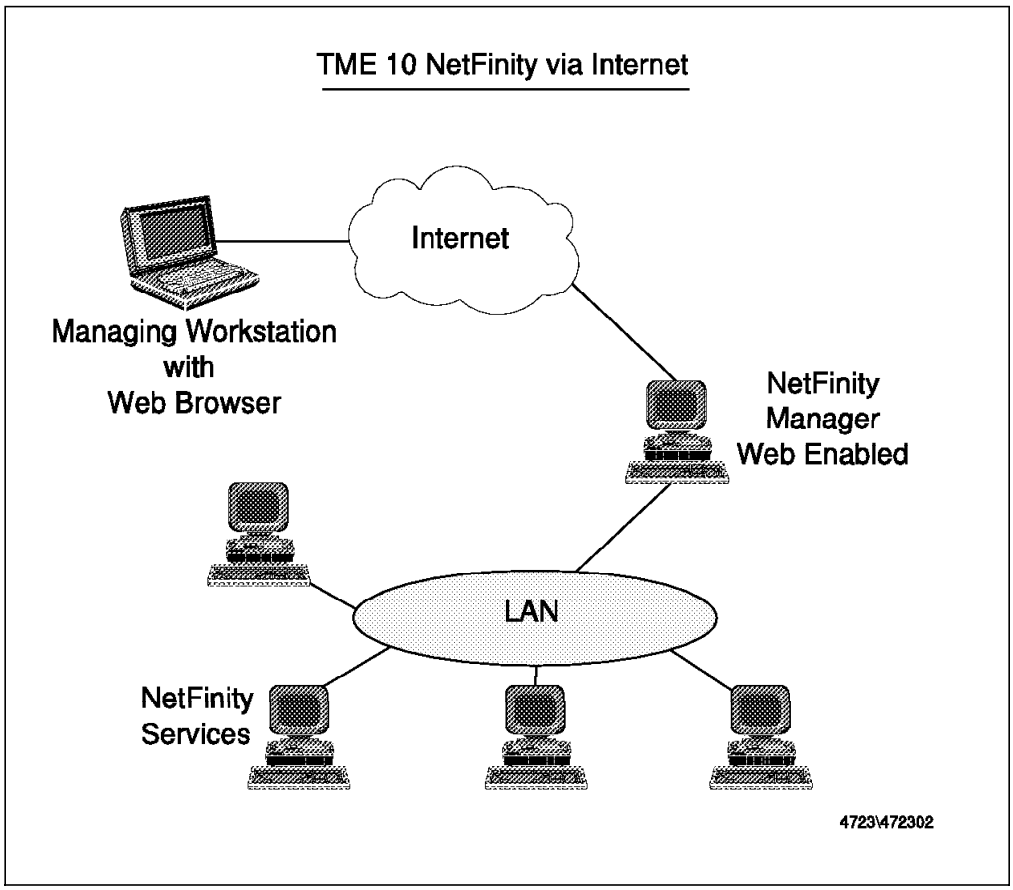


Figure 77. Internet Connection

You can monitor remote LANs via the Internet if you can connect to one station within the remote LAN that is attached to the Internet; you only need to have a Web browser installed as a managing workstation. How this can be established is shown in more detail in 6.1, “Internet Connections to TME 10 NetFinity” on page 145.

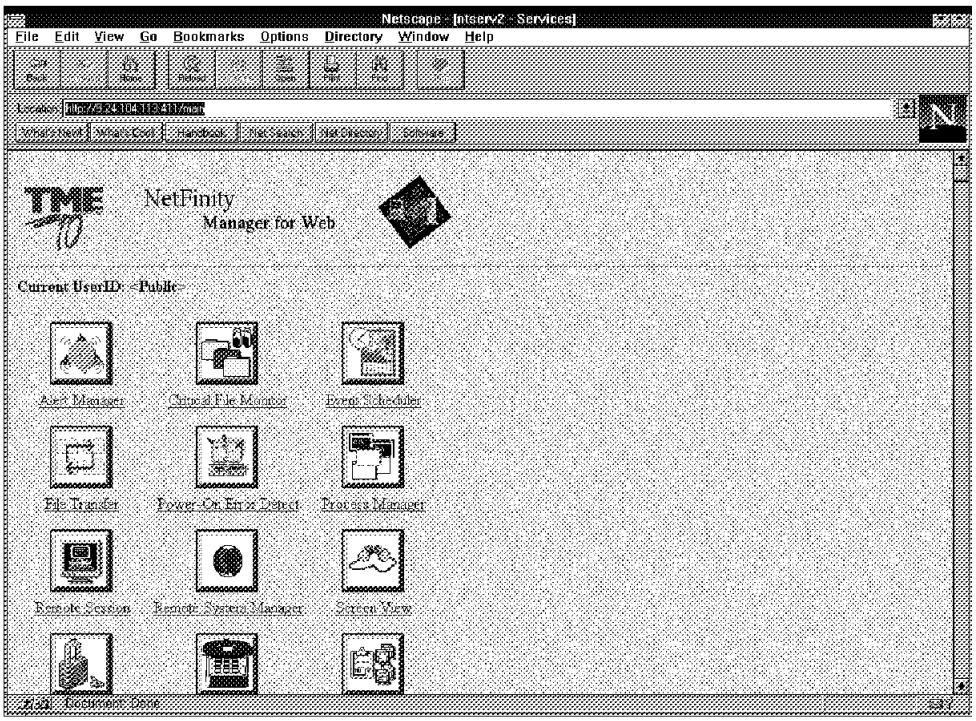


Figure 78. Web Manager Remote

Figure 78 shows the main menu when you are connected to a remote workstation via the Internet. From a functionality point of view there are very few differences if you are connected via the LAN or via the Internet. For example, the user interface for the manager looks a little different as you can see. Look in Chapter 6, “Webability” on page 145 for more details about this subject.

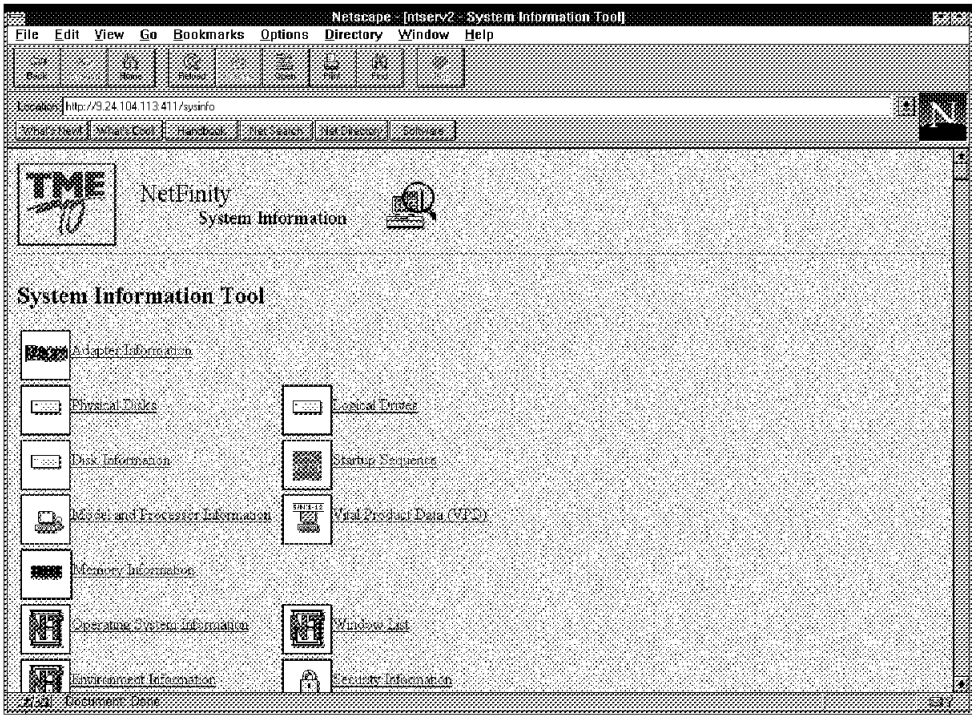


Figure 79. Web Manager - System Information

2.2 System Management Functions Provided by Windows NT

Here we describe all the different management functions available provided by NT with the appropriate menu examples and descriptions.

This part of the chapter shows examples of the built-in Windows NT systems management and monitoring functions.

2.2.1 Windows NT Disk Administrator

The local disks are administered through the Disk Administrator. The Disk Administrator shows you the physical and the logical configuration of the drives and the defined partitions.

Each physical disk is shown as a bar. The defined partitions are seen as part of the bar with different colors, depending of the type of partition.

The following functions are performed through this tool:

- Partitioning

  Disk Administrator lets you create or delete primary and extended partitions. If you define or delete partitions be aware that drive letters may change. With Windows NT you can create only one primary partition for each physical disk.

  OS/2 Boot Manager

  Do not activate an OS/2 Boot Manager partition within Windows NT. If you have both OS/2 and NT on the same machine, NT overwrites the Boot Manager record and you have to fix Boot Manager after you install NT. Changing the status of the Boot Manager partition can confuse the NT startup assignments and the system will hang during startup. To activate the Boot Manager partition after installation, start with the OS/2 boot diskettes and execute FDISK.COM.

- Assigning drive letters

  With the Disk Administrator you can change the drive letter for each partition individually. Every drive letter that is not in use can be assigned. A letter that has been in use by a drive before can be reused only after reboot.

  Individual drive letters can also be assigned to CD ROM drives.

- Defining drive arrays
  - Stripe set

    A disk stripe is the combination of free areas on two or more physical disks into one logical drive. The Disk Administrator will use an equal size on every disk. The I/O load will be balanced across all used disks.

    If you have three or more physical disks included for the stripe set, you can define disk striping with parity. This provides a possibility to have a local RAID 5 fault-tolerance system.

  - Mirror set

    A mirror set is a set of two identical partitions on two different disks combined to one logical drive. Partition one will be in real time duplicated to partition two. This lets you define a RAID 1 fault-tolerance

with either disk mirroring or, with a second disk controller, disk duplexing.

– Volume set

  A volume set is the combination of two or more various-sized areas of free space on one or more physical disks into one logical drive, treated like a single partition. This mechanism allows you to use the total available disk space more effectively.

  Volume sets can be extended dynamically by adding more unused space to the set. However, the system must be rebooted before the additional disk space is accessible.

Other OS

Be aware that other OS systems such as DOS or OS/2 do not recognize partitions within a disk set so they will not be accessible to them.

- Fault Tolerance Administration

  Through the Fault Tolerance Administration you can establish and break disk mirroring, create stripe sets with parity (RAID 5) and regenerate them after a fault occurrence.

For more information about disk managing with Windows NT, please refer to the *Windows NT Administration Guide* or to the online help.

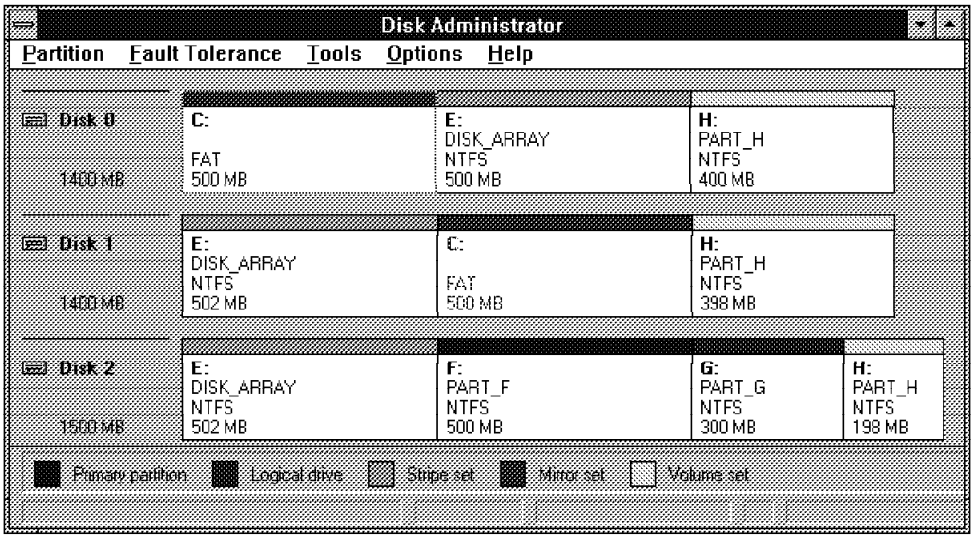


Figure 80. Windows NT Disk Administrator

The following is an explanation of Figure 80:

- Part C: is mirrored on Disk 1 and Disk 2.
- Part E: is a disk stripe set with parity.
- Part F: is a primary partition.
- Part G: is a extended partition.
- Part H: is a volume set using the remaining disk space.

Drive letter D: is used by the CD ROM drive and could not be used for a partition.

2.2.2 Windows NT Performance Monitor

Windows Performance Monitor features two main functions:

- Charting and displaying system resources
- Generating alerts according to threshold settings

This chapter covers the system resources charts. For the alert functions see 3.3, “Alerts by Windows NT Performance Monitor” on page 114.

NT Performance Monitor lets you supervise the local or remote Windows NT systems through the network.

The system resources shown can be divided into the following groups:

1. Hardware resources:
   - Physical disk
   - Processor
2. OS resources:
   - Cache
   - Logical disk
   - Memory
   - Objects
   - Paging file
   - Process
   - System
   - Tread
3. Network resources:
   - Browser
   - FTP server
   - Gateway service for NetWare
   - NBT connections
   - NetBEUI
   - NetBEUI resource
   - NWLink IPX
   - NWLink NetBIOS
   - NWLink SPX
   - ICMP
   - IP
   - TCP
   - UDP
4. Server service:
   - Redirector
   - Server

- Server work queues

5. Application resources:
   - SQL server
   - SQL server replication published DB
   - SQL server locks
   - SQL server log
   - SQL server user

This listing does not contain all possible objects. The shown objects depend on the configuration of the system.

All these objects contain multiple counters and a counter can have multiple instances. You can define a graph for every instance or, if the counter does not have multiple instances, for the counter itself.

To create a system resource chart display do the following:

1. Open **Windows NT Performance Monitor**.
2. Choose **View**; **Chart**.
3. Choose **Edit**; **Add to Chart** or click on the **+** button.
4. Select the computer name from the system you would like to supervise.
5. Select an object group.
6. Select desired counter and, if applicable, the instance.
7. Click on **Explain** for an explanation of the counter.
8. Assign a color, scale, width and style to identify the counter.

   Repeat this procedure for all counters to be shown.

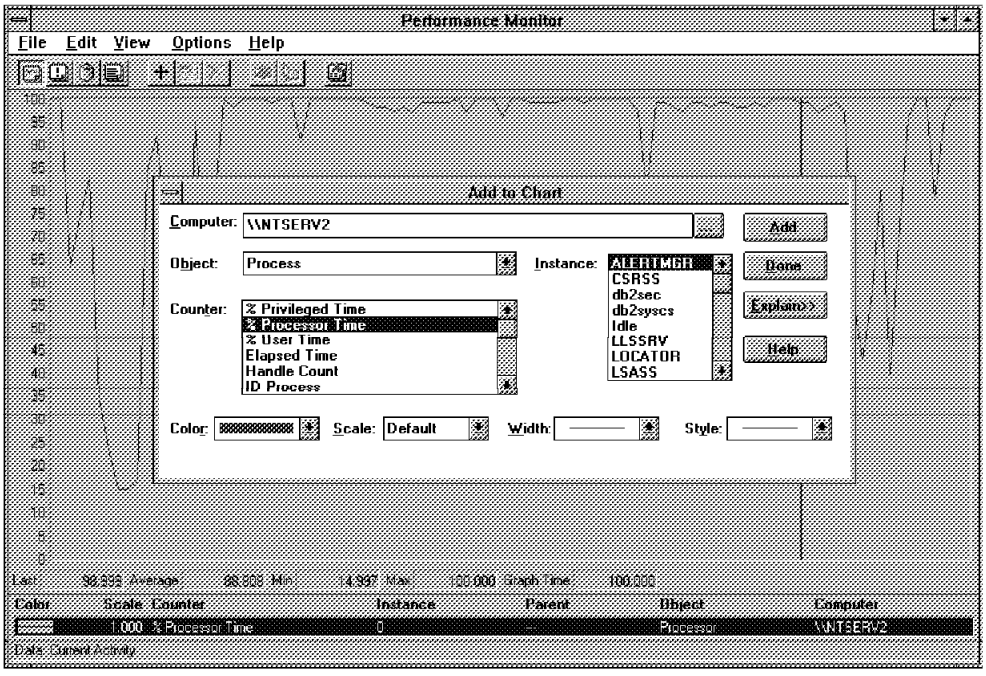


Figure 81. Windows NT Performance Monitor

2.2.3 Windows NT Server Manager

Windows NT Server Manager is used to manage systems and their resources on local or remote system within or outside the domain. Besides adding servers and workstations to the domain, promoting backup servers to primary servers and synchronizing the domain, you can do the following system administration tasks.

Before you perform any task, select the server to be managed. If the server is not in the actual domain, select **Computer**, **Select Domain** and choose the domain with the server.

- User Connections

  See all connected users and disconnect them if required.

  To open select **Computer - Properties - User**

- Shares

  See the shared resources on the server, the users using the shares and their connection time. You can also disconnect the user from a share.

  To open select **Computer - Properties - Shares**

  Add and stop shares, edit properties and permissions of a share.

  To open select **Computer - Shared Directories**

- Open Resources

  See open resources such as pipes and the users connected to them.

  To open select **Computer - Properties - In Use**

- File Replication

  Define export and import directories for file replication. The file replication service must be started and a user for file replication must be defined. See 2.2.9, “Windows NT Replication Service” on page 70.

  To open select **Computer - Properties - Replication**

- Services

  See all installed services and the status of them. You can start or stop a service from the Control Panel menu.

  To open select **Computer - Services**

- Send Messages

  Send a message to all users logged in to the managed server.

  To open select **Computer - Send Message**

To perform these actions you must be defined as domain administrator or as system administrator on the managed system.

If the FTP Service is running on the system, you can also check out the actual FTP users and their connections. Connections can be disconnected.

Note: These functions are also available for OS/2 workstations and servers, excluding share management and FTP service.

2.2.4 Windows NT Event Viewer

All events from Windows NT system and subsystems are logged in three log files:

- System log
- Security log
- Application log

The Windows NT Event Viewer is the tool to format and read these logs. They can be from the local system or from a remote system through the network.

This is the first place to check if you have any problems with the system. The entries are either Information (blue), Warnings (yellow) or Errors (red).

To see the entries in the logs do following:

- Open the **Event Viewer**.
- Select **Log** and choose one of the logs (System, Security or Application).
- Select one entry and press enter or double-click on the entry to see the details.

The logs can be saved to a file and later be reviewed. By default, the entries will be kept for seven days or until the log file reaches a certain length. To adjust these settings, select **Log** and choose **Log Settings**. The values can be set for each log file individually.

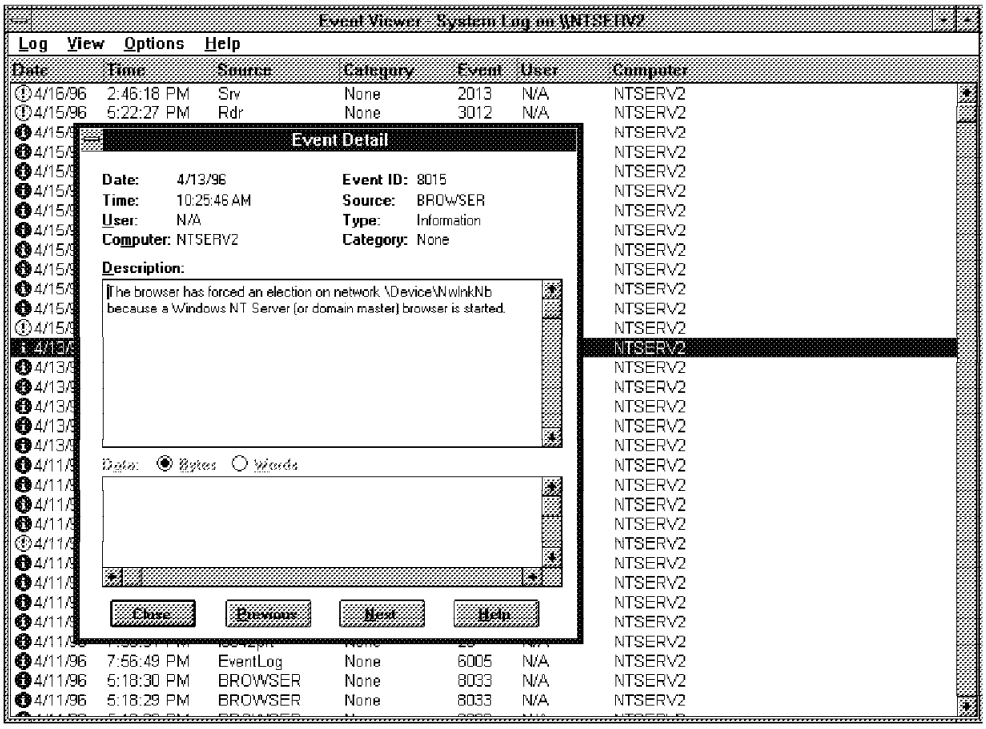

Event Viewer - System Log on \\NTSERV2
Log View Options Help
Date Time Source Category Event User Computer
4/16/96 2:46:18 PM Srv None 2013 N/A NTSERV2
4/15/96 5:22:27 PM Rdr None 3012 N/A NTSERV2
4/11/96 7:56:49 PM EventLog None 6005 N/A NTSERV2
4/11/96 5:18:30 PM BROWSER None 8033 N/A NTSERV2
4/11/96 5:18:29 PM BROWSER None 8033 N/A NTSERV2
Event Detail
Date: 4/13/96
Time: 10:25:46 AM
User: N/A
Computer: NTSERV2
Event ID: 8015
Source: BROWSER
Type: Information
Category: None
Description:
The browser has forced an election on network \Device\NwlnkNb because a Windows NT Server (or domain master) browser is started.
Data: Bytes Words
Close
Previous
Next
Help

Figure 82. Windows NT Event Viewer - Detail View

2.2.5 Windows NT Diagnostics

Windows NT Diagnostics (WINMSD.EXE) is the Windows equivalent to the MSD.EXE utility included in Microsoft products before. It analyzes the system configuration and displays the data to the user. No changes can be made to displayed values with this tool.

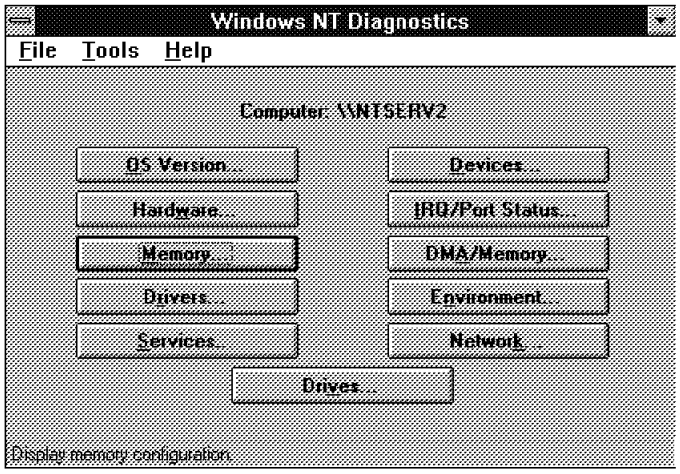


Figure 83. Windows NT Diagnostics

As you can see in Figure 83, Diagnostics shows you a lot of information about hardware, memory, drivers and much more. It lets you generate a report and send it to a printer or a file. With this tool, you can also peek at the Windows NT startup files for 16-bit applications (AUTOEXEC.NT, CONFIG.NT and WIN.INI).

This tool is mostly used by installation routines to gather information about the system and is called through an API.

Diagnostics is the best way to get fast information about the Windows NT memory and paging file status. It also displays the memory load in real time. To get this information do the following:

- Open **Windows NT Diagnostics**.
- Click on **Memory**.

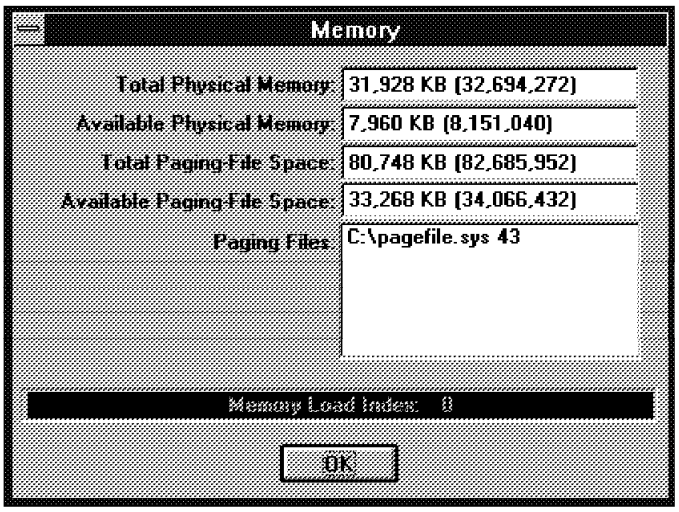


Figure 84. Windows NT Diagnostics - Memory

This utility can only be executed locally as long as it is not used in conjunction with MS Systems Management Server (SMS).

2.2.6 Windows NT Registry Editor

The Windows NT Registry is the configuration database for the entire system. Information that used to be in multiple .INI files in different places is now kept in one hierarchically database. It contains information about hardware configuration, OS environment, printer configuration, installed software and much more. Almost all 32-bit application relay on this database. There are still some .INI files for compatibility to 16-bit windows applications.

In most cases database entries are handled by the Windows NT itself or by software installation routines.

Caution!

Because database fields can be various types like ASCII, binary or hex, it is not always simple to handle this values manually. Faulty entries can cause system malfunctions or even force a system reinstallation in the worst case. Be very carefully by altering values manually and do nothing until you understand fully the consequences of your change. Always back up your registry using a tool like the regback command, that comes with the NT Resource Kit.

With the Windows NT Registry Editor you can edit this database on the local system or on remote system through the network. To perform any changes you must have administrative rights within the domain the system belongs to or on the system itself. You can also be given certain rights on keys as on file objects.

The Registry Editor has no icon in the Program Manager by default. You can start the Registry Editor either by typing REGEDT32 in a command box or create a Program Manager icon by dragging and dropping REGEDT32.EXE from the File Manager to the desired Program Manager group. REGEDT32.EXE is located in the SYSTEM32 subdirectory of the Windows NT program directory.

The registry is divided in different hives, one for the system configuration (HKEY_LOCAL_MACHINE) and one for the user profiles (HKEY_USERS). These hives are hierarchically structured and every level can have values and/or one or more sublevels assigned.

The Windows NT Registry Editor displays four hives by default:

- HKEY_LOCAL_MACHINE
- HKEY_USERS
- HKEY_CLASSES_ROOT (subtree of HKEY_LOCAL_MACHINE)
- HKEY_CURRENT_USER (subtree of HKEY_USERS)

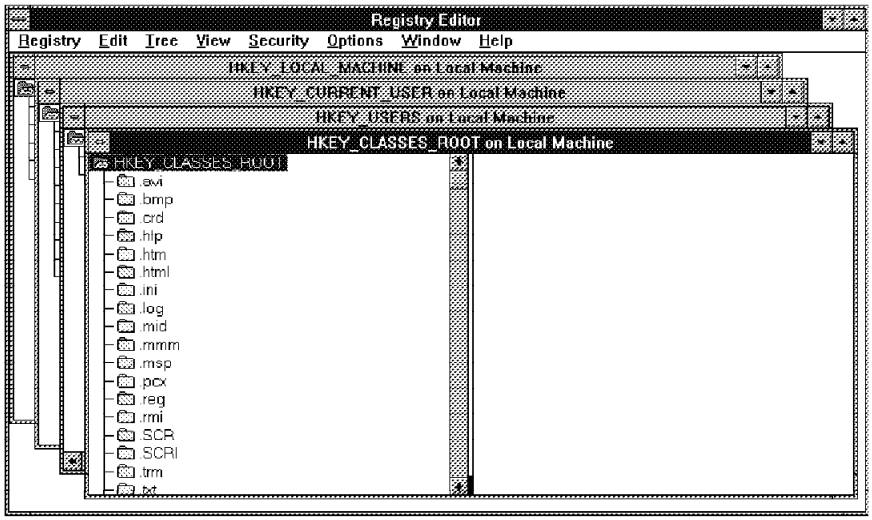


Figure 85. Windows NT Registry Editor - Default View

If you select the registry of another computer through the network, only the main hives (HKEY_LOCAL_MACHINE and HKEY_USERS) will be displayed.

The HKEY_USERS tree contains all data related to a certain user. If a user is logging in to a system for the first time, a copy of the default profile will be made and a unique user ID assigned. If users make any changes to their environment, the changes will be saved in this profile. In the HKEY_USERS tree, only the default user and the user actually logged on to the managed system are displayed. All other user profiles are hidden and not accessible.

If you change any values in this hive, it will only affect this certain user or, if you make the changes in the default profile, all newly created users.

The HKEY_LOCAL_MACHINE tree has five distinct subtrees:

Hardware	Contains all hardware configuration data, device drivers, device and resource maps.
SAM	System internal key; can not be edited.
Security	(Grayed out) System internal key; can not be edited.
Software	Contains the information for object linking and embedding, configuration data for applications, system services, the Program Manager configuration and migration data.

System Contains Windows NT setup information, a control set for each found system configuration and the current control set with the current configuration values.

In the hardware and software branch of the tree, you normally don't have to edit entries. These are made through the installation and configuration program. In the software branch you might found some values that can be changed manually to alter the settings for an application.

Please consult the Help function to get more information about adding keys, adding or editing values and the different value types. Make sure you enter values in the right format.

2.2.6.1 Backup and Restore the Registry

Within the Registry Editor, you can save every key with its subkeys to a file except the Security key, were only the system has the rights to access. You can not save entire hives.

With the restore function of the Registry Editor, Keys with its subkeys can be restored to its original hive as long as the active key is not in use. Open Keys can not be overwritten.

The Registry function of backup and restore is suitable to save individual keys for backup reasons or to use them on other systems. You can not use it to back up the whole system configuration. For this, there are two possibilities:

- Back up the system with the Windows NT Tape Backup program to a tape drive. This will back up the registry hives even when they are in use. Also the restore task will override the active registry. The restores registry entries will be active after rebooting the system.
- If you don't have a tape drive or not want to use it, there are tools delivered with the Windows NT Resource Kit to back up (REGBACK.EXE) and restore (REGREST.EXE) entire hives. There are also more tools to handle the registry. See 2.3, "System Management Tools Provided by Windows NT Resource Kit" on page 74 about using the NT Resource Kit.

2.2.6.2 Entries by TME 10 NetFinity

TME 10 NetFinity Manager and Agent makes its own entries into the software branch of the HKEY_LOCAL_MACHINE. We found the following entry:

```
HKEY_LOCAL_MACHINE
  |
  |-- Software
  |      |
  |      |-- IBM
  |      |     |
  |      |     |-- NetFinity (TME 10 NetFinity Version dll-File)
  |      |
  |      |-- ProgramGroups
  |            |
  |            |-- NetFinity (The TME 10 NetFinity Program Group)
  |
  |
  |-- System
         |
         |-- ControlSetxxx / CurrentControlSet (content in all Control sets)
               |
               |-- Services
                     |
                     |-- EventLog
                     |     |
                     |     |-- Application
                     |           |
                     |           |-- NetFinity (For entries in the Application log file)
                     |
                     |-- Netfbase (TME 10 NetFinity Support Program)
```

2.2.7 Windows NT Dr. Watson Utilities

Dr. Watson (DRWATSON.EXE) is a diagnostic utility that detects system and application failures (for example, general protection (GP) faults) and stores Windows internal data in a file called DRWATSON.LOG. Certain areas of this file may be useful when troubleshooting problems that may exist.

2.2.7.1 How to Read a Dr. Watson Log

The Dr. Watson log is divided into sections, with each section being separated by a blank line.

- The start (and stop) line records the time and date that Dr. Watson was started. A series of start lines indicates Windows with no application errors. A start line immediately followed by a stop line indicates the same thing.
- The failure report line records the time and date when the error occurred. It also tells which version of Dr. Watson was running at the time.
- The next two lines are related. The line ″< APPLICATION NAME> had a <fault description> fault at <module name> <cs: ip register>″ is a descriptive way of stating the next line (the tag line). The tag line divides the error into fields separated by ″$″. The first field indicates what application you were in when the error occurred. The second field indicates the probable error. The third field indicates which module probably caused the error, and its memory location. The fourth field is the instruction in the

stack that the application was on when the error occurred. The fifth field is the time/date that the error occurred.

- The next two log sections indicate what was in the various CPU registers at the time of failure. The 32-bit registers are listed separately in the second register section.
- The System Info section provides information about the system and Windows. User name and Organization are taken from Windows .INI files.
- The Stack Dump section is divided into frames. You can find out what was in the stack before the fault occurred in this section, in the first frame (0), by locating its memory location in the stack. The memory location was indicated in the third field of the tag line.
- The final section lists the applications running from the tasks list. The number of tasks running can be found in the System Info section.

A user description appears at the end of the log. These lines are preceded by a #> (for example, 1>, 2>, and so on).

2.2.7.2 Troubleshooting with Dr. Watson

The Dr. Watson log file is intended for debugging purposes. The more Windows NT knowledge you have, the more useful the Dr. Watson log file will be. At the very least, it can help isolate what application and module caused the error. In general it is more important which module caused the error than the application you were in when the error occurred. For example, the following log in the failure report section shows an error that could have been associated with the display driver:

```
Dr. Watson 0.80 Failure Report- Wed Apr 17 16&colon42&colon34 1996
Write had a 'Code Segment (Read)' fault at Display 2: ld70
$tag$WRITE$Code Segment (Read)$Display 2: ld70$mov
```

In this example, the program that caused the error message was Write and the module is Display. The first troubleshooting step in this case would be to test Write while using a different video driver.

It is important to remember that Dr. Watson is a diagnostic tool, and not a cure for a problem. Having Dr. Watson will not prevent an error from occurring, but the information in DRWATSON.LOG can help isolate the problem.

2.2.8 Windows NT License Management

Windows NT Server has its own License Management built in. This can handle the client access licenses of the Microsoft BackOffice products installed in the network. Microsoft BackOffice Products are NT Server, MS SQL Server, MS SNA Server and Systems Management Server (SMS).

The purchase of any product able to access the MS Server Products does not automatically include a client access license. For example, Windows 95 does not include a license to access a Windows NT Server. For every server product, an access license must be purchased separately except with the BackOffice Client Access License which includes all server products.

Microsoft has two different license agreements:

- License by server
- License by seat

With the License by Server you buy for each server a certain amount of client access licenses and configure them on the server. The amount must match the maximum of concurrent user connections to this server. Multiple connections from one client to the server count as one connection. This type of licensing makes the most sense if users do not connect to multiple servers or do not change servers often.

If you choose to license the clients by seat, the amount of clients in the whole network counts. Once a client claims its license within the network, it will be acknowledged by all other servers of the same kind. The license information will be replicated among all defined servers within the network. You can define one enterprise server to manage all client licenses. This server can even be in another domain.

Note

If you are not sure which type of licensing you should define during the first installation, choose License by Server. There is a one-way option to change to the License by Seat mode later.

2.2.8.1 The Windows NT License Manager

Microsoft Licensing allows you to define the number of client access licenses, according to your license agreement. It manages only the Microsoft BackOffice Products (Windows NT Server, MS SQL Server, MS SNA Server and MS Systems Management Server). Other products or programs shared by file server can not be accounted for with Microsoft Licensing.

To account for the licenses within the network, use the Microsoft License Manager on a Windows NT Server. You start the License Manager from the Network Administration group.

From the License Manager windows you can choose four different views:

- **Purchase History:** Provides a history listing of all actions taken to add or remove product licenses.

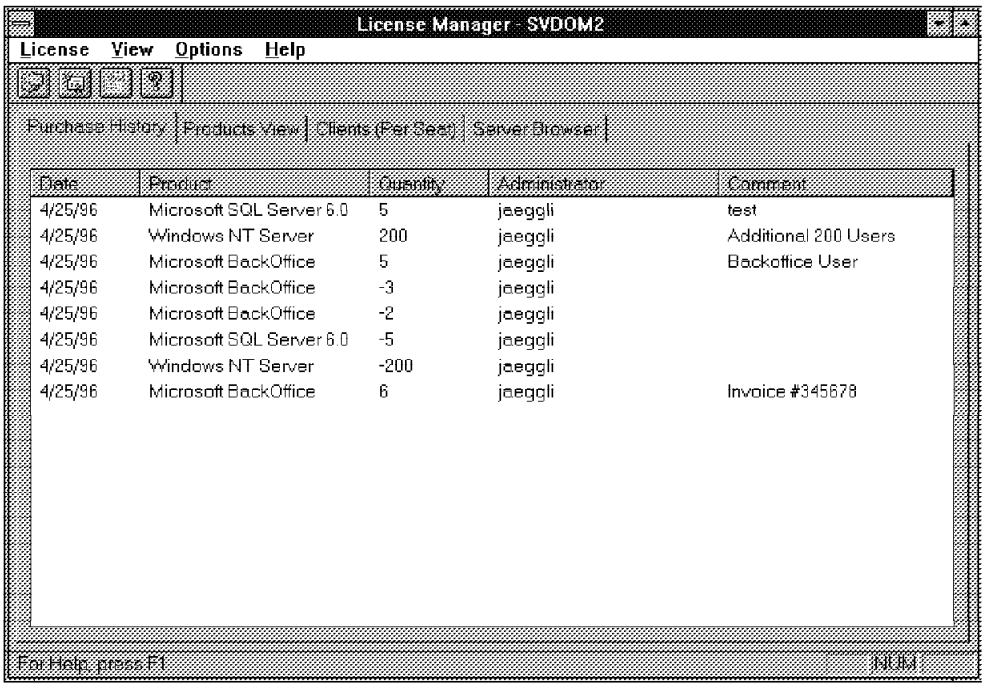

License Manager - SVDOM2
License View Options Help
Purchase History | Products View | Clients (Per Seat) | Server Browser
Date | Product | Quantity | Administrator | Comment
4/25/96 Microsoft SQL Server 6.0 5 jaeggli test
4/25/96 Windows NT Server 200 jaeggli Additional 200 Users
4/25/96 Microsoft BackOffice 5 jaeggli Backoffice User
4/25/96 Microsoft BackOffice -3 jaeggli
4/25/96 Microsoft BackOffice -2 jaeggli
4/25/96 Microsoft SQL Server 6.0 -5 jaeggli
4/25/96 Windows NT Server -200 jaeggli
4/25/96 Microsoft BackOffice 6 jaeggli Invoice #345678
For Help, press F1
NUM

Figure 86. License Manager - Purchase History

This is only an information page. Entries can't be modified nor deleted. If you add or delete licenses, a new entry will be made.

- **Product View:** Gives you an overview of the installed products, the licenses per mode and how many times accessed. It also shows how the defined number of licenses compares with the actually number of claimed licenses.

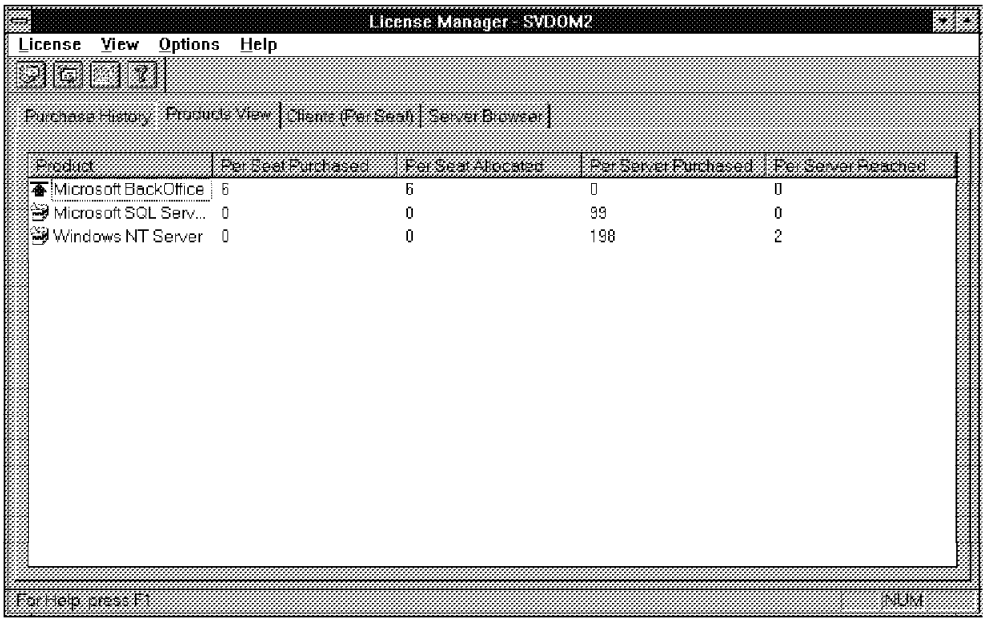

License Manager - SVDOM2
License View Options Help
Purchase History | Products View | Clients (Per Seat) | Server Browser
Product | Per Seat Purchased | Per Seat Allocated | Per Server Purchased | Per Server Reached
Microsoft BackOffice 6 6 0 0
Microsoft SQL Serv... 0 0 99 0
Windows NT Server 0 0 198 2
For Help, press F1
NUM

Figure 87. License Manager - Product View

Double-click on the product name to see the system/user name that accessed the product and the purchase history for this product. With the server browser see on which systems this product runs.

- **Clients (per seat):** Shows the workstation and user name that accessed a product and if a license is provided or not.

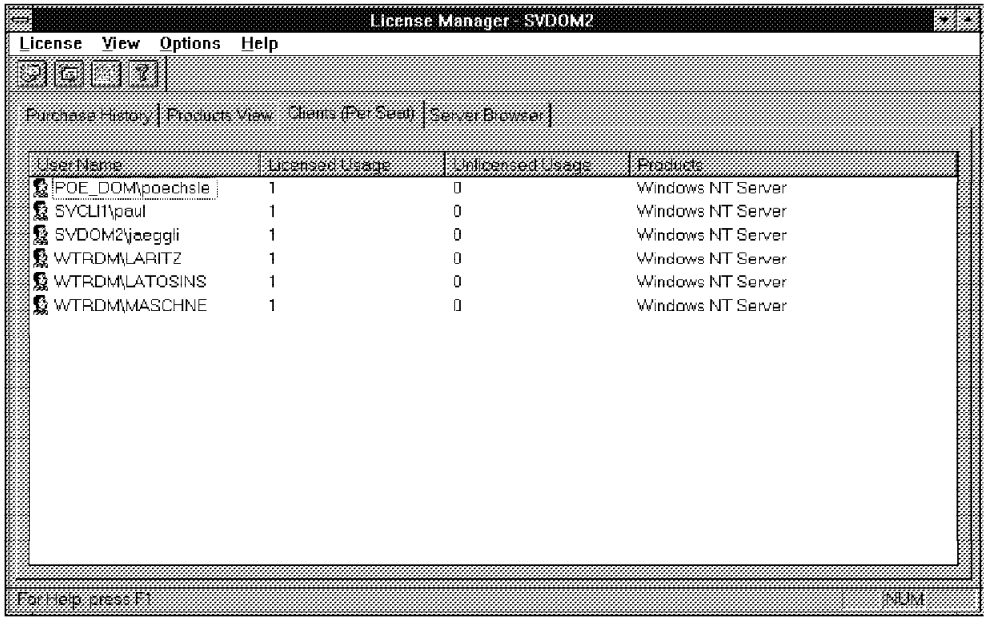

License Manager - SVDOM2
License View Options Help
Purchase History Products View Clients (Per Seat) Server Browser
User Name Licensed Usage Unlicensed Usage Products
POE_DOM\poechsle 1 0 Windows NT Server
SVCLI1\paul 1 0 Windows NT Server
SVDOM2\jaeggli 1 0 Windows NT Server
WTRDM\LARITZ 1 0 Windows NT Server
WTRDM\LATOSINS 1 0 Windows NT Server
WTRDM\MASCHNE 1 0 Windows NT Server
For Help, press F1
NUM

Figure 88. License Manager - Clients

This page shows you all accounted clients and if they have assigned a license or not. Double-click on the system/user name to revoke or upgrade the license.

- **Server Browser:** Displays a tree view of all found domains and their servers with a licensing service running.

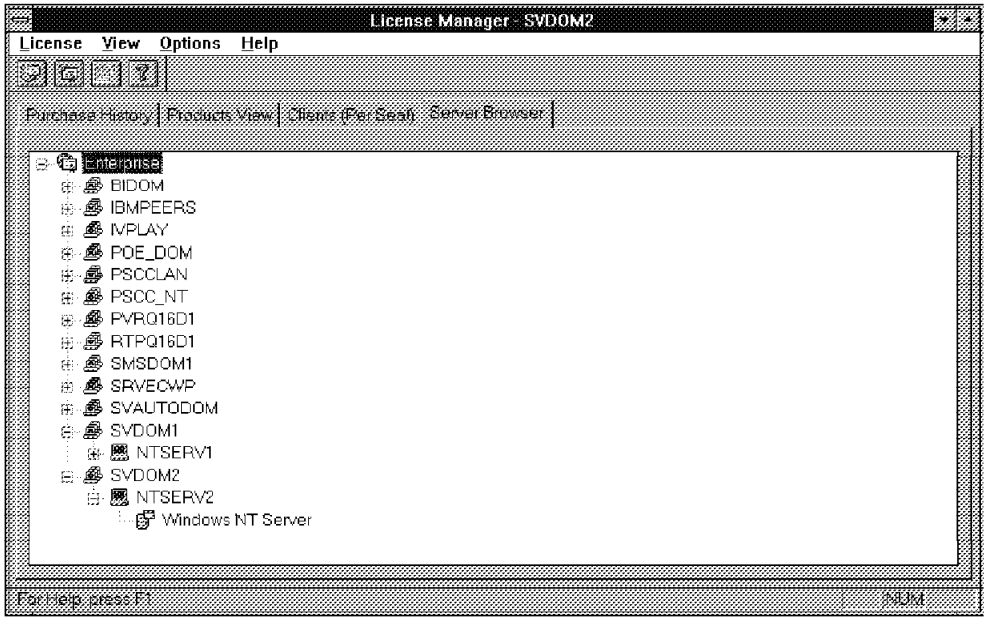


Figure 89. License Manager - Server Browser

Expand the tree until all license servers are displayed. Double-click on the server object and set the license mode and, if license mode by server is chosen, the amount of license. In this section, it is possible to change the

license mode from *by seats* to *by server*. The Microsoft documentation does inform you that this it is not legal to do this.

You can always add a license by clicking on the New License button or choosing **License**, **New License** from the top menu.

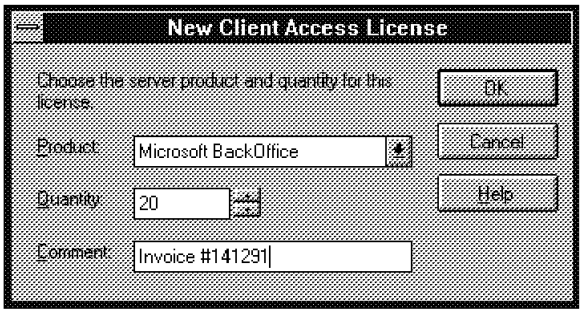


Figure 90. License Manager - New Client Access License

Choose the product to add licenses, set the amount of new purchased licenses and add a comment. Click on **OK** to activate the new licenses.

2.2.8.2 The Licenses Applet in the Control Panel

This applet is used to configure the amount of client access licenses or to choose the licensing mode for the local system. Do the following to configure systems licenses:

1. Open the **Windows NT Control Panel** from the Program Manager and start the Licensing Program.
2. Select the desired product.
3. Enter the amount of licenses according to the license agreement if you work by server.
4. Or, select the radio button **Per Seat** if you want change the licensing mode

   If you select License by Seat, you have to configure the replication for the license accounting.
5. Click on **Replication** to open the replication definition window.
6. Select the server to handle the license accounting and define a time to replicate the license information.
7. Click on **OK** to activate the settings and close windows.

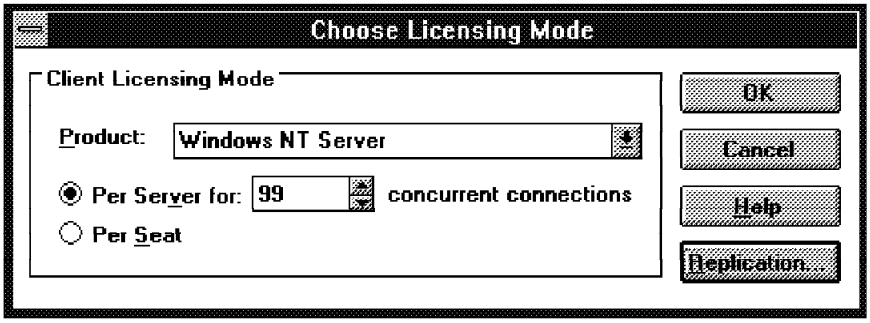


Figure 91. Choose Licensing Mode

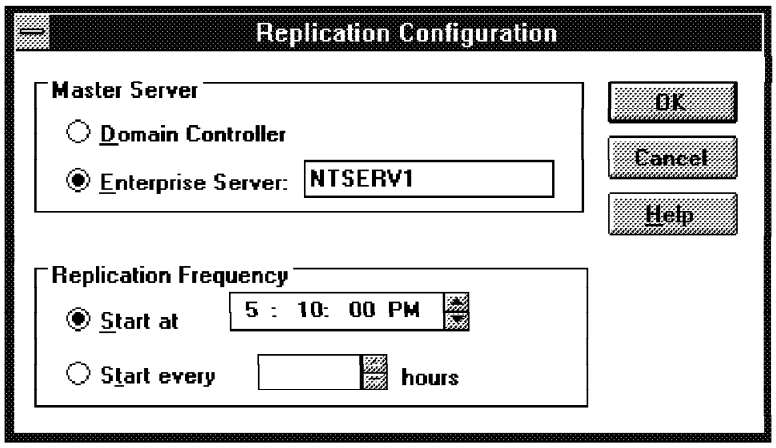


Figure 92. License Replication Configuration

2.2.9 Windows NT Replication Service

Windows NT provides a service to replicate files and directories from a system to one or more other systems. The sending system is called the export server and the receiving system is the import server. The export server is checking the defined export directory for new, deleted or changed files in regular intervals. If it encounters a change, the import directories of the import server will be updated.

Windows NT server supports export and import functions. NT workstations only support the import function. NT servers can also export and import from/to an OS/2 LAN server. By exporting files from one file system to another (for example from NTFS to FAT), the file names must meet both systems requirements.

You can define one export and one import directory per server. These directories can contain 32 subdirectories with 1024 files each at most.

2.2.9.1 Export Service

To configure the export service do the following:

1. Create a user account for the Replication service.
   - Start **NT User Manager** from the Administrative Tools group.
   - Create an account for the Replication service. Use a user name related to the replication service and set a password. De-select the check box User Must Change Password at Next Logon.

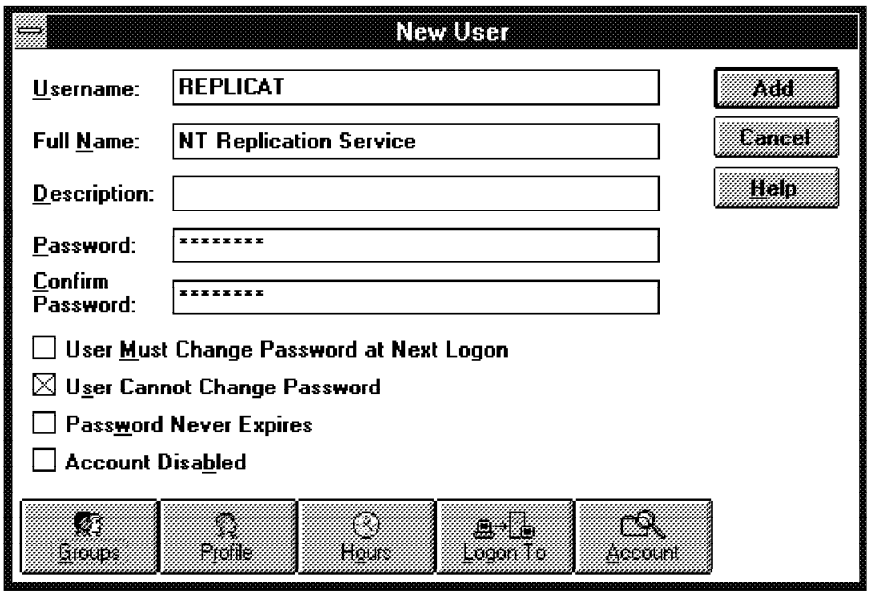


Figure 93. NT User Manager - New User

- Click on the **Groups** button and put the new user into the replicator group by selecting **Replicator** from the Not Member of window and click on the **Add** button.

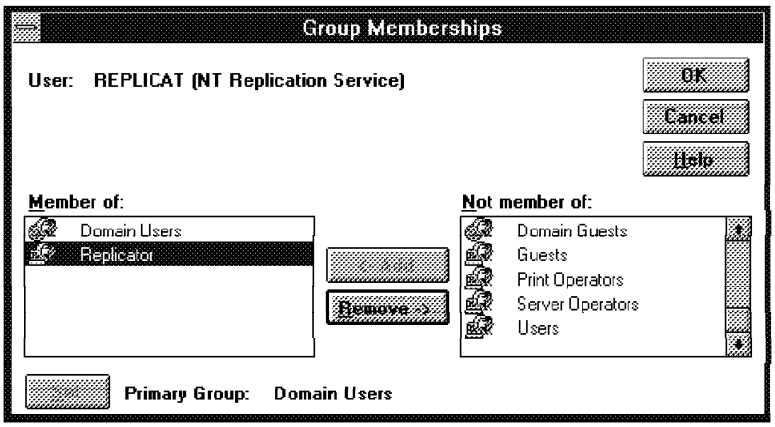


Figure 94. NT User Manager - Group Membership

- Click on **OK** to close the Group Membership window.
- Click on **Add** to add the user to the database.
- Click on **OK** to close the New User window.
- Close NT User Manager.

2. Configure the Replication Service.
   - Open the **Services** applet in the system control panel.
   - Select **Directory Replicator** and click on the **Startup** button.
   - Set Startup Type to Automatic.
   - Select the **This Account** radio button in the Log On As window and enter the name of the just created replicator account. Make sure you insert the same password that was created during the account creation.

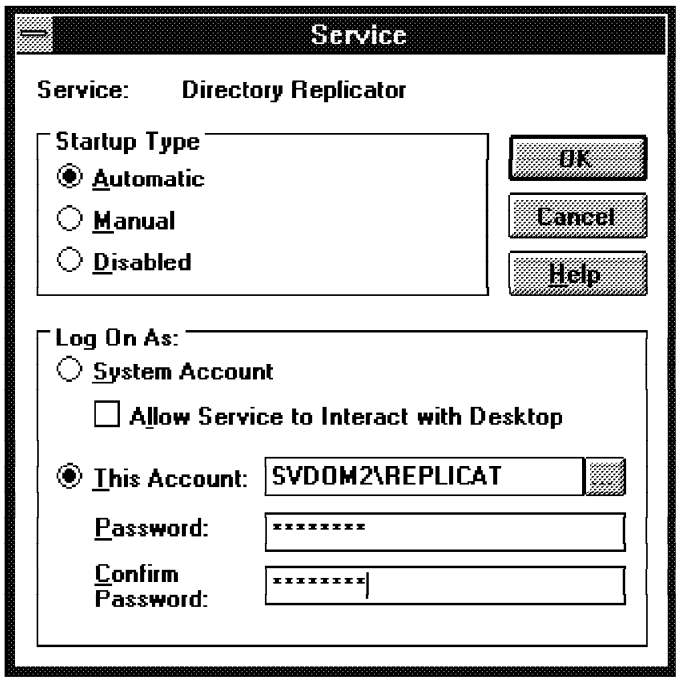


Figure 95. Service Manager - Service Configuration

- Click on **OK** to close the window. A message that replicator status has been granted to the service should be shown.
- Click on **Start** to start the Replicator Service.
- Close the Services window when the replicator has been started successfully.

3. Configure the export directories.
   - Start the Server Manager from the Administrators Tool group.
   - Select the system with the export server service and choose **Computer** and **Properties** from the top menu.
   - Click on the **Replication** button.
   - Select the directory to be replicated.

     By default, the \WINNT\SYSTEM32\REPL\EXPORT directory is selected. This directory with its subdirectory \SCRIPTS is normally used for the replication of logon scrips. If your workstations use LAN Manager logon scripts from this server, do not alter the path.
   - Click on **Add** to add the names of import server or domains.

     If you enter a domain name, the directories will be exported to all systems in this domain, running the import service.

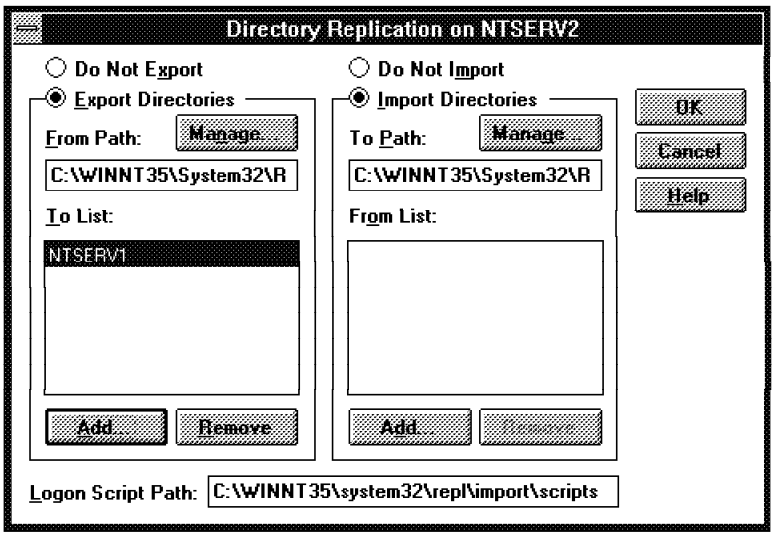


Figure 96. NT Server Manager - Directory Replication

- Click on the **Manage** button to add, configure or remove subdirectories.

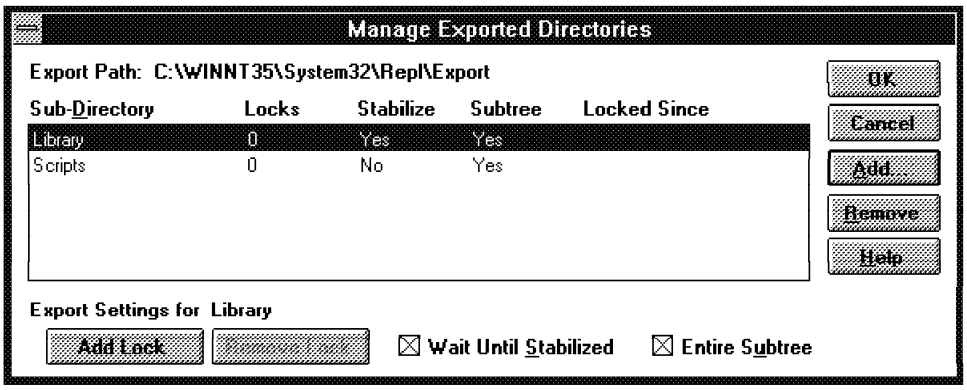


Figure 97. NT Server Manager - Manage Exported Directories

- Add, edit or delete directories. Click on **Help** for more information about the function of each setting.
- Click the **OK** button three times to close the windows and leave the NT Server Manager.

2.2.9.2 Import Service

To configure the Import service do the following:

1. Perform the same two steps that were done when configuring the Export service.
2. Start the Server Manager from the Administrators tools group.
3. Select the system you wish to configure the import service for and choose **Computer** and **Properties** from the top menu.
4. Click on the **Replication** button.
5. Select the directory to be imported.

   By default, the \WINNT\SYSTEM32\REPLY\IMPORT directory is selected. This directory with its subdirectory \SCRIPTS is normally used for the replication

of logon scrips. If the system you are configuring acts as a logon server with LAN Manager logon scripts, do not alter this path.

6. Click on **Add** to add names of one or more export servers.

   By default, the import services imports from the local domain manager. If you make any entries in this list, files will be imported only from the listed servers.

7. Click on the **Manage** button to add, configure or remove subdirectories to be imported.

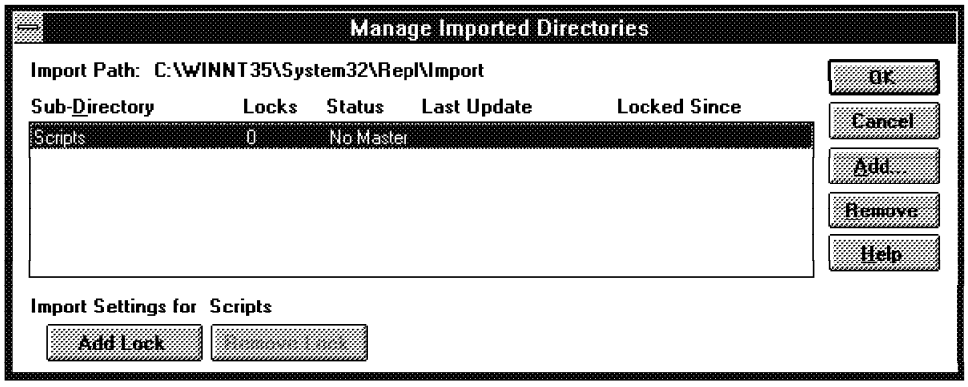


Figure 98. NT Server Manager - Manage Imported Directories

8. Add, edit or delete directories. Click on **Help** for more information about the function of each setting.

9. Click the **OK** button three times to close the windows and leave the NT Server Manager.

2.3 System Management Tools Provided by Windows NT Resource Kit

The Windows NT Resource Kit is a collection of tools and utilities to support the administration of Windows NT Systems and networks. It can be purchased separately or found on the Microsoft Technet CD-ROMs. It contains programs, documents and help files. It even contains tools for multiple purposes within NT System Administration. We showed only a few of them in this book. The ones we think are the most usable in relation to system administration in a network environment were selected.

After the installation of the Resource Kit, the following new program group is shown.

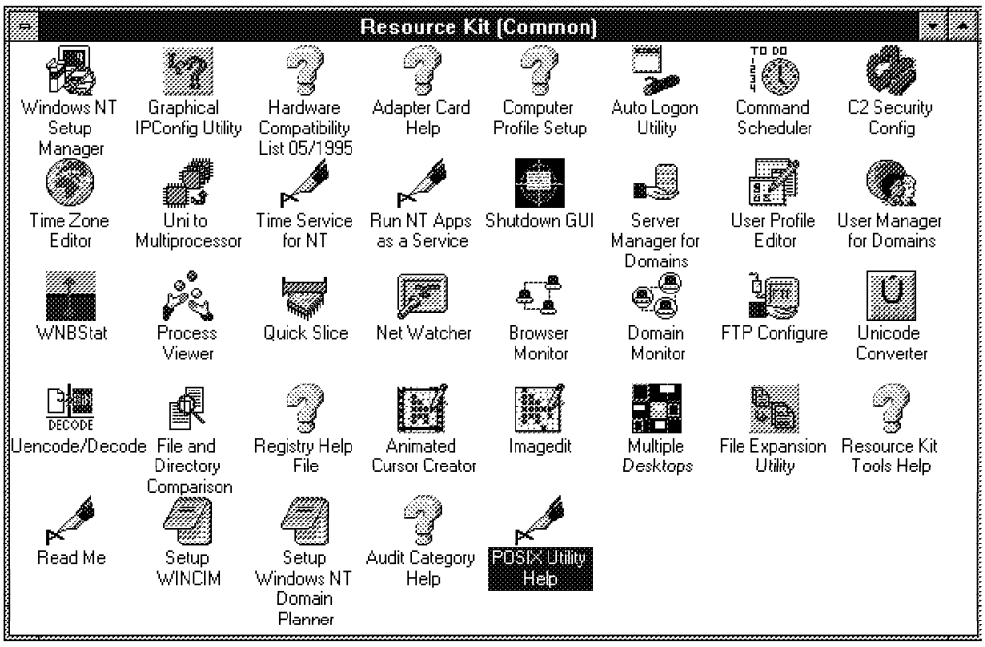


Figure 99. Windows NT Resource Kit - Program Group

With the installation of the Windows NT Resource Kit, additional utilities, not shown in the program group, are copied to the root directory of the Resource Kit. To get more information about these tools, click on the **Resource Kit Tools Help** push button from the Resource Kit group. This help utility contains the descriptions and explanations for all delivered tools and programs. Select the desired book, browse through the index or search a specific word with the search function. All the following tools and programs are referred within this help tool.

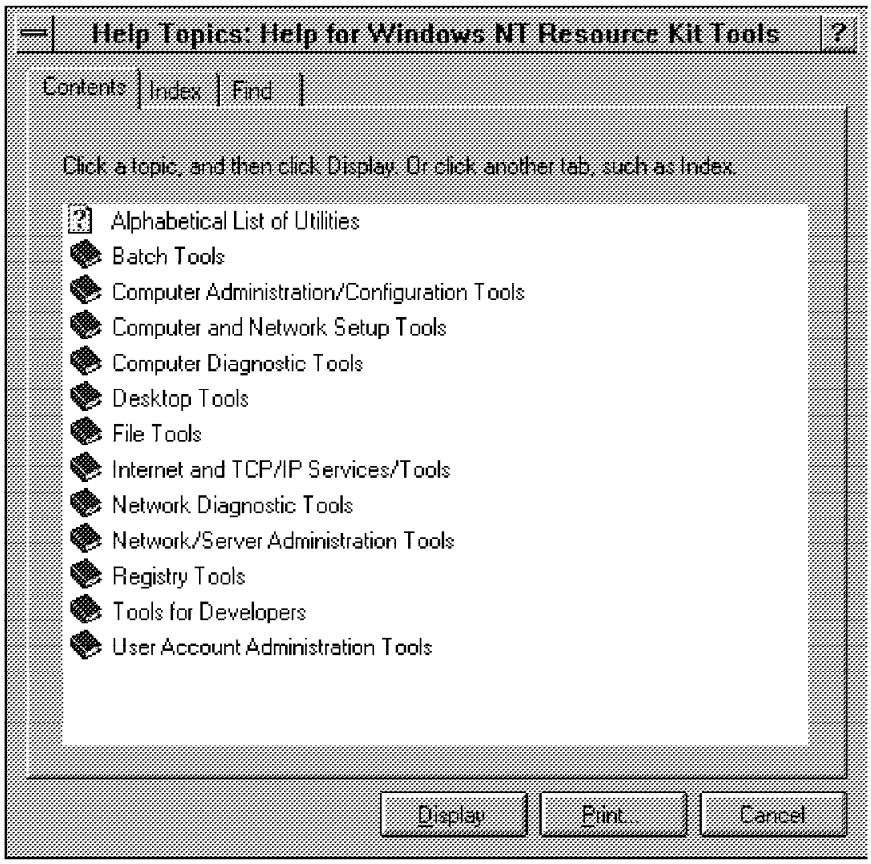


Figure 100. Windows NT Resource Kit - Resource Kit Tools Help

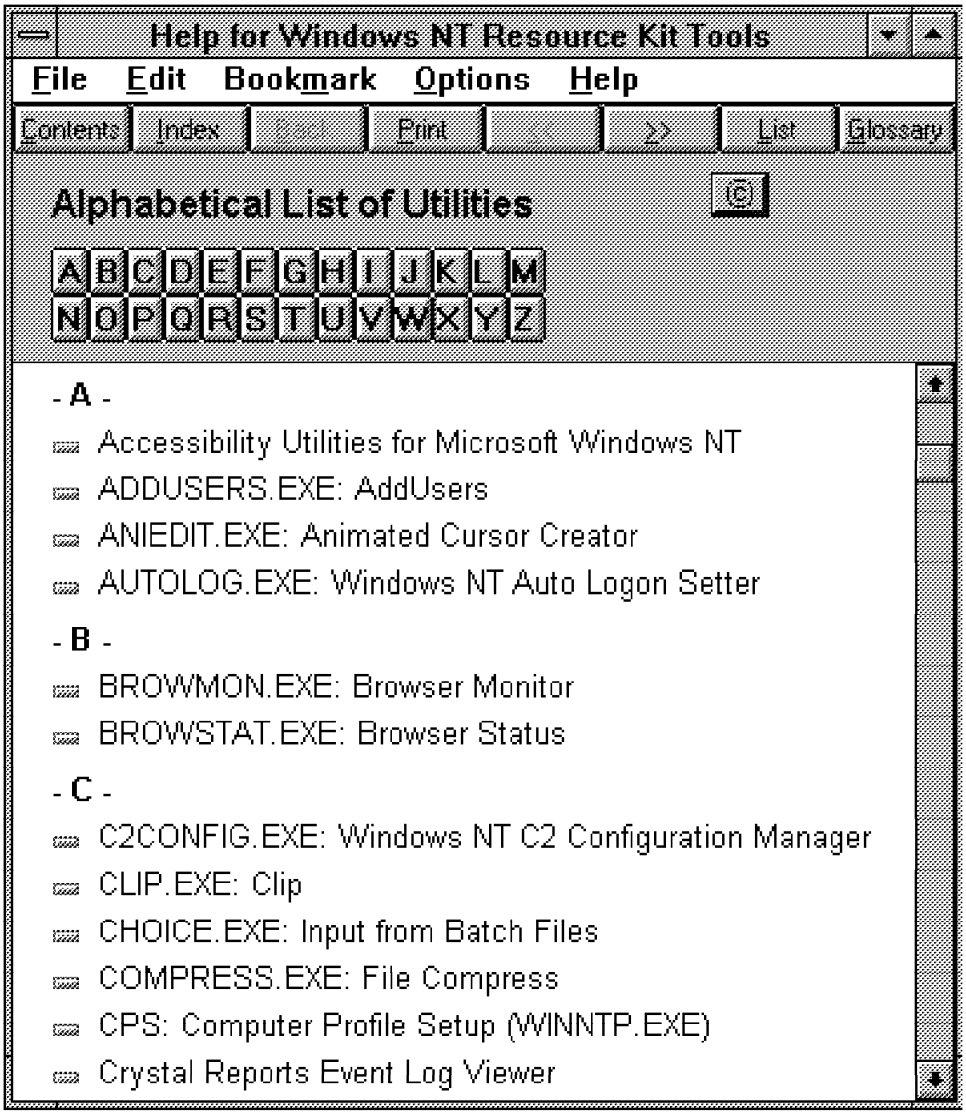

Help for Windows NT Resource Kit Tools
File Edit Bookmark Options Help
Contents Index Print << List Glossary
Alphabetical List of Utilities
A B C D E F G H I J K L M
N O P Q R S T U V W X Y Z
- A -
Accessibility Utilities for Microsoft Windows NT
ADDUSERS.EXE: AddUsers
ANIEDIT.EXE: Animated Cursor Creator
AUTOLOG.EXE: Windows NT Auto Logon Setter
- B -
BROWMON.EXE: Browser Monitor
BROWSTAT.EXE: Browser Status
- C -
C2CONFIG.EXE: Windows NT C2 Configuration Manager
CLIP.EXE: Clip
CHOICE.EXE: Input from Batch Files
COMPRESS.EXE: File Compress
CPS: Computer Profile Setup (WINNTP.EXE)
Crystal Reports Event Log Viewer

Figure 101. Windows NT Resource Kit - Utilities

2.3.1 Automatic Login and Shutdown Management

The NT Resource Kit provides several utilities that help with automating logins and shutdowns of NT.

2.3.1.1 Automatic Login

With the Windows NT Autologon Setter (AUTOLOG.EXE) utility you can set Windows NT to log on a user automatically at startup. You have to provide the user ID and the password.

This tool changes the following registry entry: HKEY_LOCAL_MACHINE/ Software/Microsoft/Windows NT/CurrentVersion/Winlogon. It adds the Key AutoAdminLogon=1 and DefaultPassword=the entered Password to this hive.

To activate the automatic logon do the following:

1. Log on to Windows NT with the user ID the system should log on automatically.

2. Start AUTOLOG.EXE or double-click on the Auto Logon Utility in the Resource Kit window.
3. Enter the password into the Password field as shown in Figure 102.
4. Click on **OK** to perform the changes in the Registry.

To stop the system from automatically logging on do the following:

1. Start **AUTOLOG.EXE**.
2. Choose the **Remove Auto Logon** radio button.
3. Click on **OK** to perform the changes in the registry.

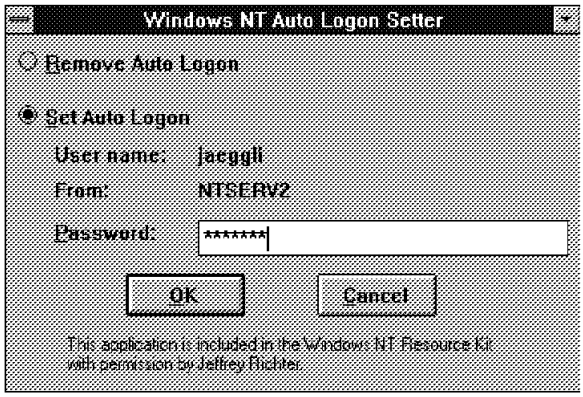


Figure 102. Windows NT Auto Logon Setter

Warning

If any error message occurs during logon (for example a drive could not be mapped), the system will wait for interaction and not continue the logon process.

2.3.1.2 Shutdown Manager GUI (SHUTGUI.EXE)

The Shutdown Manager provides a graphical user interface to shut down and restart a local or remote Windows NT system.

Choose the computer name of the system to be rebooted, how much time to wait before rebooting and enter a message to be displayed to the system user.

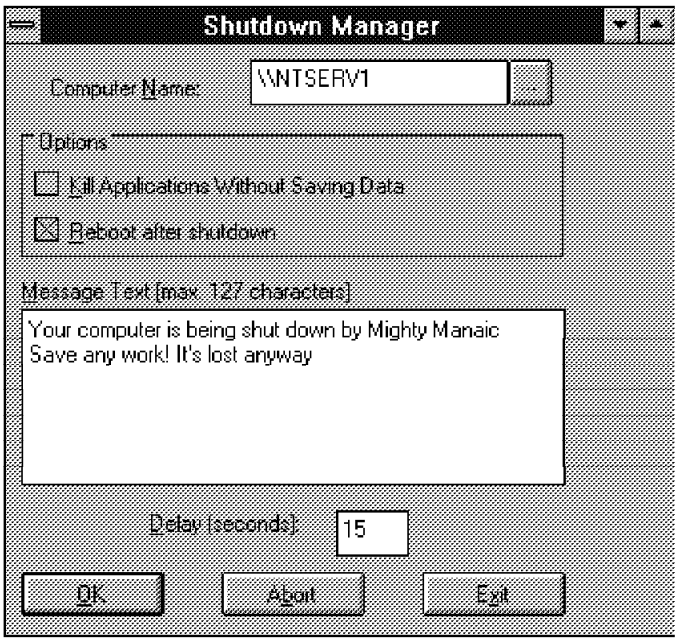


Figure 103. Shutdown Manager (GUI)

2.3.1.3 Shutdown Manager Command (SHUTCMD.EXE)

The Shutdown Manager command provides the same functions as the GUI utility, but it can be used in a batch program with the following parameters:

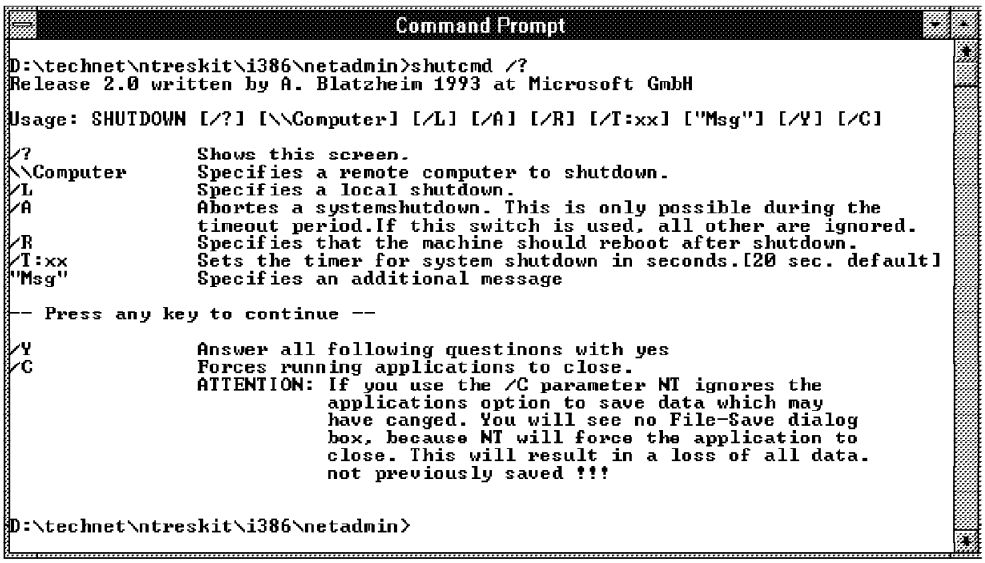

Command Prompt
D:\technet\ntreskit\i386\netadmin>shutcmd /?
Release 2.0 written by A. Blatzheim 1993 at Microsoft GmbH
Usage: SHUTDOWN [/?] [\\Computer] [/L] [/A] [/R] [/T:xx] ["Msg"] [/Y] [/C]
/? Shows this screen.
\\Computer Specifies a remote computer to shutdown.
/L Specifies a local shutdown.
/A Abortes a systemshutdown. This is only possible during the
timeout period.If this switch is used, all other are ignored.
/R Specifies that the machine should reboot after shutdown.
/T:xx Sets the timer for system shutdown in seconds.[20 sec. default]
"Msg" Specifies an additional message
-- Press any key to continue --
/Y Answer all following questinons with yes
/C Forces running applications to close.
ATTENTION: If you use the /C parameter NT ignores the
applications option to save data which may
have canged. You will see no File-Save dialog
box, because NT will force the application to
close. This will result in a loss of all data.
not previously saved !!!
D:\technet\ntreskit\i386\netadmin>

Figure 104. SHUTCMD.EXE - Help Screen

You can use the shutcmd command in an automated process to reboot systems after performing some system maintenance.

2.3.2 Process Management

2.3.2.1 Process Viewer (PVIEWER.EXE)

The Process Viewer shows you all of the currently running processes and their threads on the desired Windows NT system. You can also see the memory details of the process/thread.

If the select process is running on the local system, you can change its task priority or kill the process.

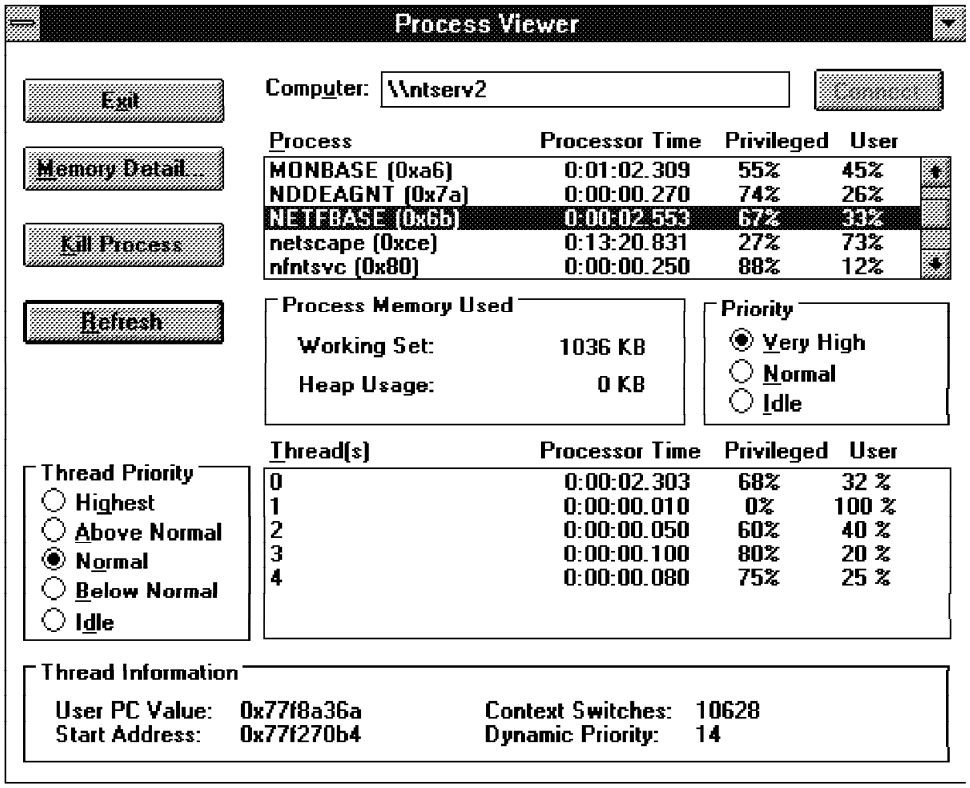


Figure 105. Process Viewer

The process shown in Figure 105 is from TME 10 NetFinity.

2.3.2.2 The Tools TLIST.EXE and KILL.EXE

These are two command line programs that look at the running processes and kill a process if needed. TLIST.EXE displays all running processes on the system with their process ID. This process ID is used as a parameter with KILL.EXE to kill the process.

Run the programs with the parameter **/?** to get more instructions about using these utilities or see the Resource Kit help utility.

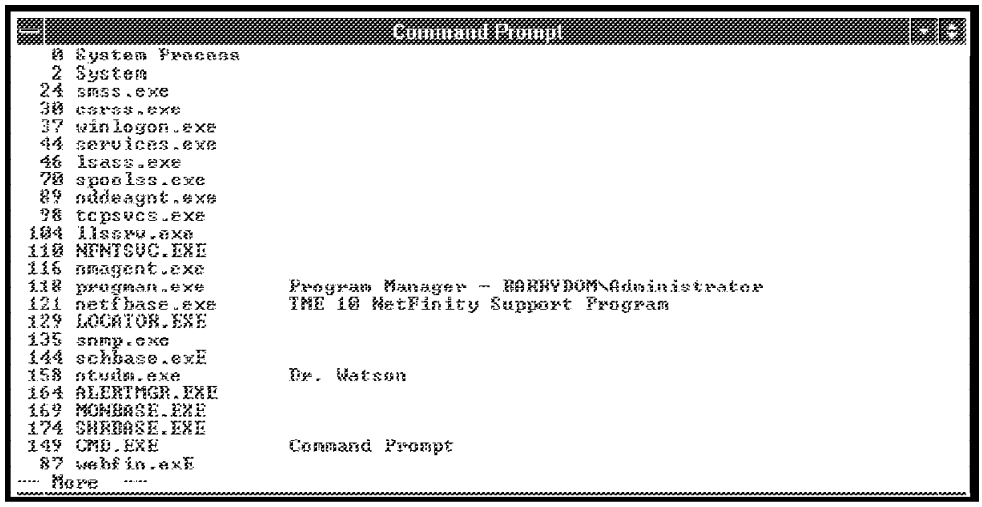


Figure 106. TLIST.EXE Output

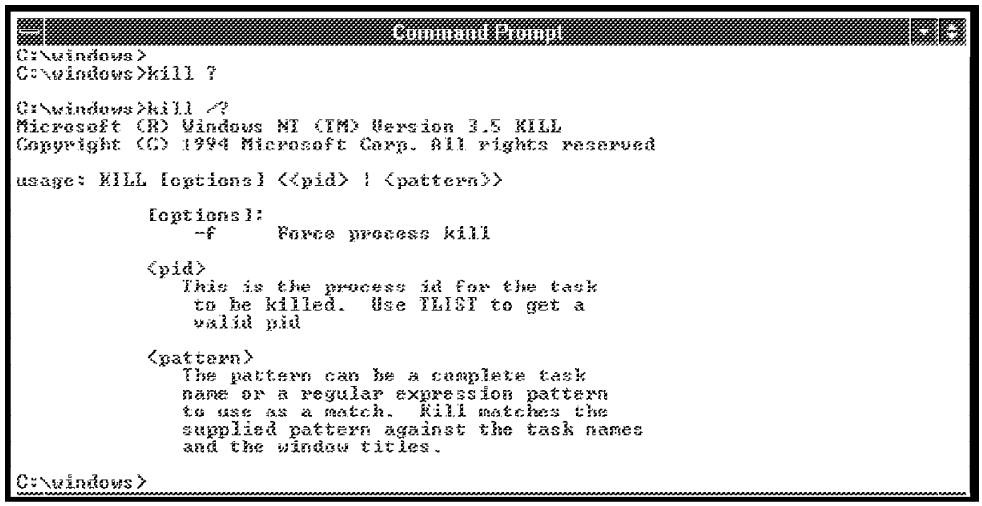

Command Prompt
C:\windows>
C:\windows>kill 7
C:\windows>kill /?
Microsoft (R) Windows NT (TM) Version 3.5 KILL
Copyright (C) 1994 Microsoft Corp. All rights reserved
usage: KILL [options] <<pid> | <pattern>>
[options]:
-f Force process kill
<pid>
This is the process id for the task
to be killed. Use TLIST to get a
valid pid
<pattern>
The pattern can be a complete task
name or a regular expression pattern
to use as a match. Kill matches the
supplied pattern against the task names
and the window titles.
C:\windows>

Figure 107. TLIST.EXE Output

2.3.2.3 Process Statistics PSTAT.EXE

PSTAT.EXE displays all running processes on the system with a process ID (PID), priority and handles. There is also a line for every thread belonging to the process with the thread ID (TID), the assigned priority and the status of the thread.

Run the programs with the parameter ***/?*** to get more instruction about using these utilities or see the Resource Kit help utility.

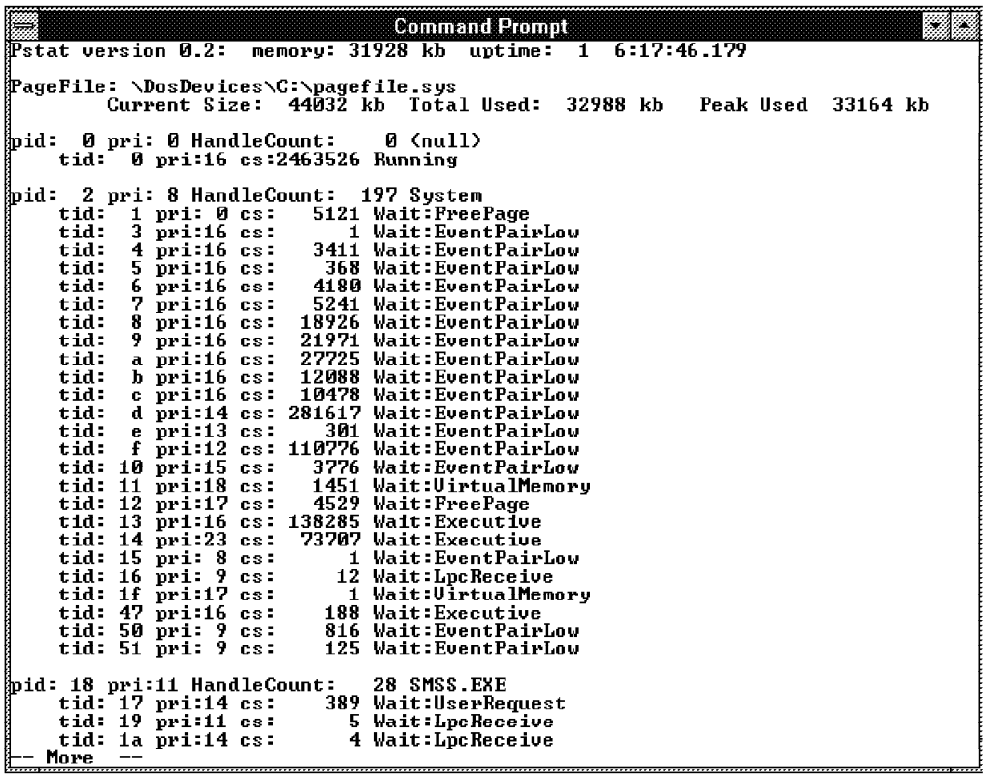

Command Prompt
Pstat version 0.2: memory: 31928 kb uptime: 1 6:17:46.179
PageFile: \DosDevices\C:\pagefile.sys
Current Size: 44032 kb Total Used: 32988 kb Peak Used 33164 kb
pid: 0 pri: 0 HandleCount: 0 (null)
tid: 0 pri:16 cs:2463526 Running
pid: 2 pri: 8 HandleCount: 197 System
tid: 1 pri: 0 cs: 5121 Wait:FreePage
tid: 3 pri:16 cs: 1 Wait:EventPairLow
tid: 4 pri:16 cs: 3411 Wait:EventPairLow
tid: 5 pri:16 cs: 368 Wait:EventPairLow
tid: 6 pri:16 cs: 4180 Wait:EventPairLow
tid: 7 pri:16 cs: 5241 Wait:EventPairLow
tid: 8 pri:16 cs: 18926 Wait:EventPairLow
tid: 9 pri:16 cs: 21971 Wait:EventPairLow
tid: a pri:16 cs: 27725 Wait:EventPairLow
tid: b pri:16 cs: 12088 Wait:EventPairLow
tid: c pri:16 cs: 10478 Wait:EventPairLow
tid: d pri:14 cs: 281617 Wait:EventPairLow
tid: e pri:13 cs: 301 Wait:EventPairLow
tid: f pri:12 cs: 110776 Wait:EventPairLow
tid: 10 pri:15 cs: 3776 Wait:EventPairLow
tid: 11 pri:18 cs: 1451 Wait:VirtualMemory
tid: 12 pri:17 cs: 4529 Wait:FreePage
tid: 13 pri:16 cs: 138285 Wait:Executive
tid: 14 pri:23 cs: 73707 Wait:Executive
tid: 15 pri: 8 cs: 1 Wait:EventPairLow
tid: 16 pri: 9 cs: 12 Wait:LpcReceive
tid: 1f pri:17 cs: 1 Wait:VirtualMemory
tid: 47 pri:16 cs: 188 Wait:Executive
tid: 50 pri: 9 cs: 816 Wait:EventPairLow
tid: 51 pri: 9 cs: 125 Wait:EventPairLow
pid: 18 pri:11 HandleCount: 28 SMSS.EXE
tid: 17 pri:14 cs: 389 Wait:UserRequest
tid: 19 pri:11 cs: 5 Wait:LpcReceive
tid: 1a pri:14 cs: 4 Wait:LpcReceive
-- More --

Figure 108. PSTAT - Listing

2.3.3 Performance Monitoring

2.3.3.1 Performance Monitor PMON.EXE

PMON.EXE lists out all running processes with memory usage, CPU usage and also an overview off the overall system load. The screen is updated approximately every 5 seconds. If not all processes are shown, change the properties of the command prompt box to display more lines.

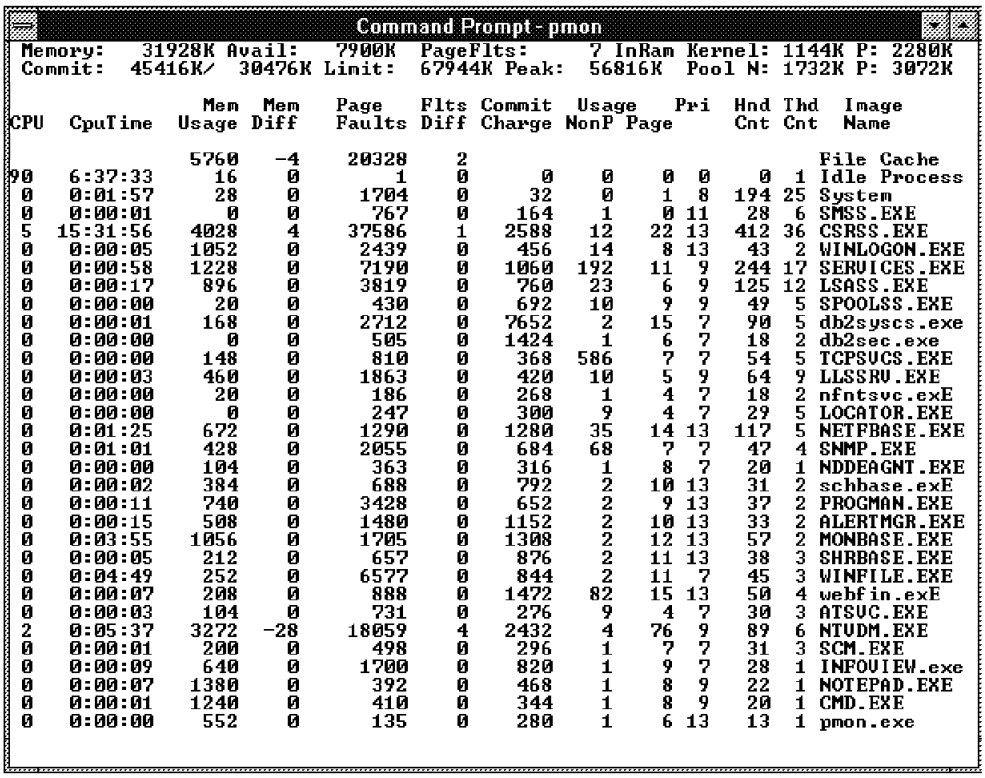


Figure 109. Performance Monitor - PMON.EXE

2.3.3.2 QuickSlice Process Monitor QSLICE.EXE

QuickSlice displays all active processes with the process ID and their CPU usage in real time in a graphical interface.

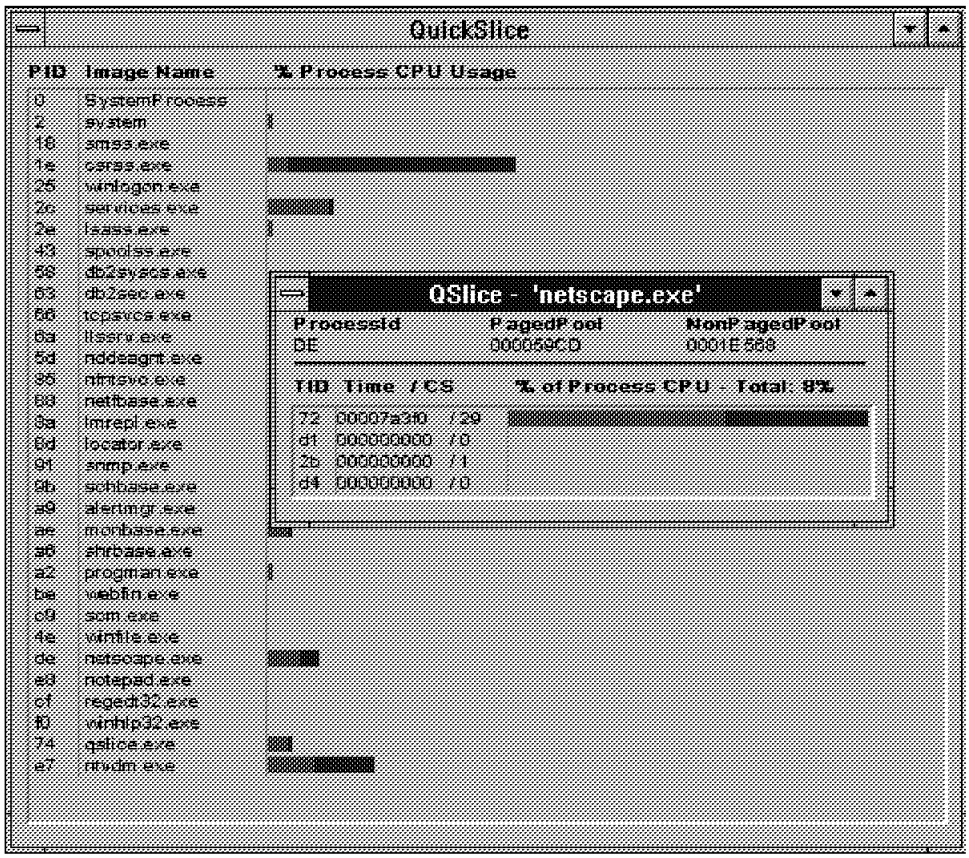


Figure 110. QuickSlice Process Monitor QSLICE.EXE

The QuickSlice window shows two bars per process:

- Red bar = kernel time
- Blue bar = user time

By double-clicking on the image name, a second window is shown with the threads and their CPU usage. Figure 110 has the thread window in the middle of it.

For the main window, the length of the bar represents:

```
(CPU usage for a single process) / (CPU usage for all processes currently running in the system) * 100
```

For the secondary windows, the length of the bar represents (CPU usage for an individual thread) / (CPU usage for all the threads in this process) * 100.

2.3.4 Command Scheduler

For command scheduling, Windows NT provides the AT command. With Windows NT comes the old AT command line command, known from MS LAN Manager or IBM LAN Server. It still has the same function: start a Command at a certain time and date. There are some enhancements within the Windows NT command:

- The parameter \\COMPUTERNAME was added to set and change AT schedules on remote computers through the network.
- The parameter /INTERACTIVE was added. This allows the job to interact with the desktop of the user who is logged on at the time the job runs.

For more information about the usage of the AT command type AT /? in a command line box. You will get a window like the following:

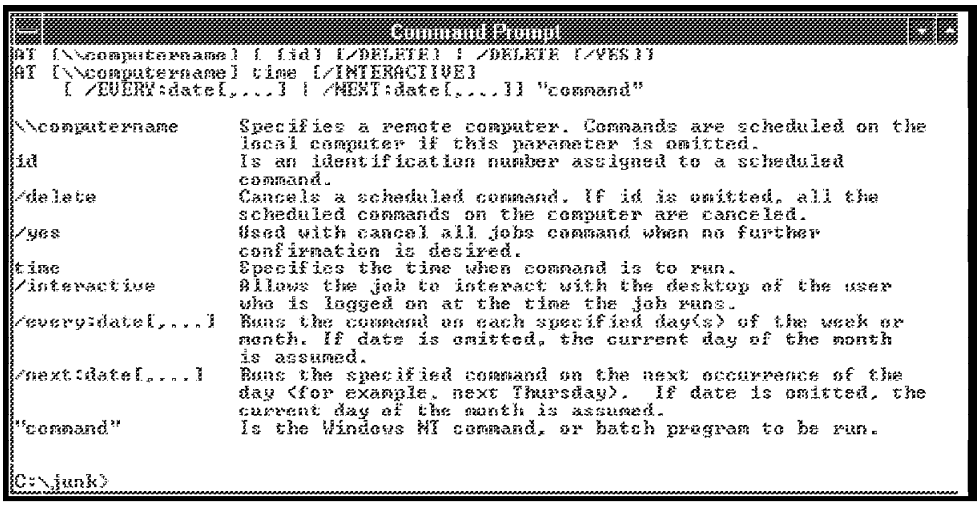

Command Prompt
AT [\\computername] [id] [/DELETE] | /DELETE [/YES]]
AT [\\computername] time [/INTERACTIVE]
[/EVERY:date[,...] | /NEXT:date[,...]] "command"
\\computername Specifies a remote computer. Commands are scheduled on the local computer if this parameter is omitted.
id Is an identification number assigned to a scheduled command.
/delete Cancels a scheduled command. If id is omitted, all the scheduled commands on the computer are canceled.
/yes Used with cancel all jobs command when no further confirmation is desired.
time Specifies the time when command is to run.
/interactive Allows the job to interact with the desktop of the user who is logged on at the time the job runs.
/every:date[,...] Runs the command on each specified day(s) of the week or month. If date is omitted, the current day of the month is assumed.
/next:date[,...] Runs the specified command on the next occurrence of the day (for example, next Thursday). If date is omitted, the current day of the month is assumed.
"command" Is the Windows NT command, or batch program to be run.
C:\junk>

Figure 111. Fields for the AT Command

With the Windows NT Resource Kit comes a graphical user interface to set, change or delete job schedules. The program name is WINAT.EXE. The Command Scheduler displays the current settings and allows you to create a new job and delete or change an existing job.

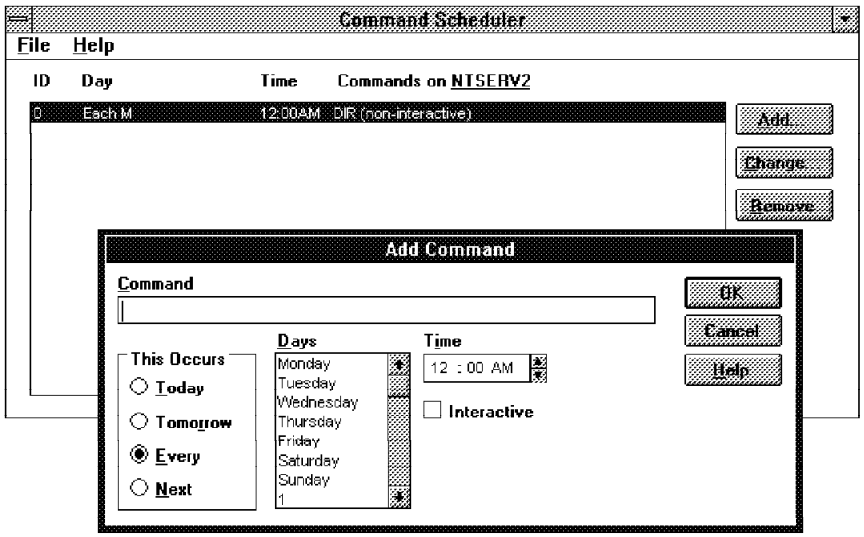


Figure 112. Command Scheduler GUI

Before you can access the job scheduling database of a system, the scheduler service must be started and you must have the rights to add or perform changes to scheduled jobs. To start the scheduler service remotely, see 2.2.3, “Windows NT Server Manager” on page 58.

2.3.5 Network and Domain Monitoring

2.3.5.1 Net Watch

Net Watch (NETWATCH.EXE) lets you supervise one or more NT systems (server or workstation) in the network, shows you the shares and resources to be shared and, if they are in use, by which user they are accessed in a tree view. By double-clicking on an object with the right mouse button and choosing **Properties**, more detailed information can be seen.

Depending on the configuration of Net Watch it shows all open files and the hidden shares or only shares currently in use. Set the configuration through the Options menu.

If you have selected to see the open files, the path to the directory where the open files reside and the file names are shown. However, an icon that looks like a pair of eyeglasses marks files that are opened in read mode and an icon that looks like a pen marks those that are open in read/write mode.

Also by clicking on the right button of the mouse on the object, you can either remove the computer from the display, stop sharing a resource, disconnect a user from a resource or close a resource, depending on the object type.

The Net Watch window can be configured to always stay on the display. Mark in the **Options** menu **Always on top** with a check sign.

From the Connection menu you can connect and disconnect network drives (as you would do in the File Manager) or select other computers to supervise. To delete a computer from display just select the computer and press Delete.

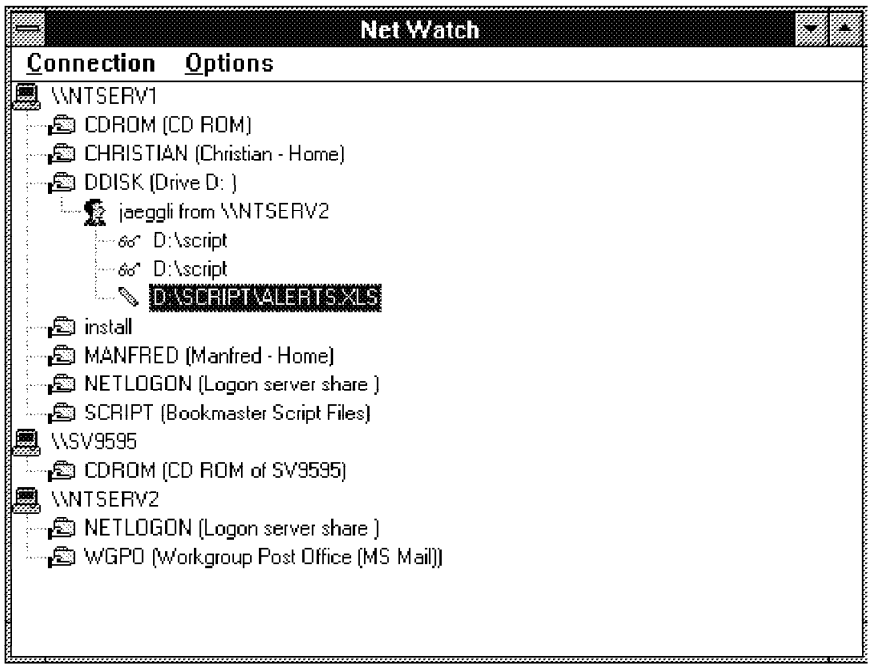


Figure 113. Net Watch (NETWATCH.EXE)

No NT systems using SMBs (for example OS/2 Peer or Server) may be included in the monitoring since errors may occur.

2.3.5.2 Browser Monitor

In every Windows NT domain as well as in Windows NT, Windows 95, Windows for Workgroup workgroups is one system, the master browser. Within domains, usually the domain controller supports this function. In workgroups, the first system joining a workgroup becomes the master browser. The master browser allows all other systems within or outside the domain to browse through the systems and their resources known by the browser database. For every configured network, a master browser is established. The master browser maintains a list of all systems that who have announced themselves in the domain on a specific network transport protocol and another list of all other domains found on that protocol.

The Browser Monitor shows you the domain name, the network transport protocol and the system name with the master browser function.

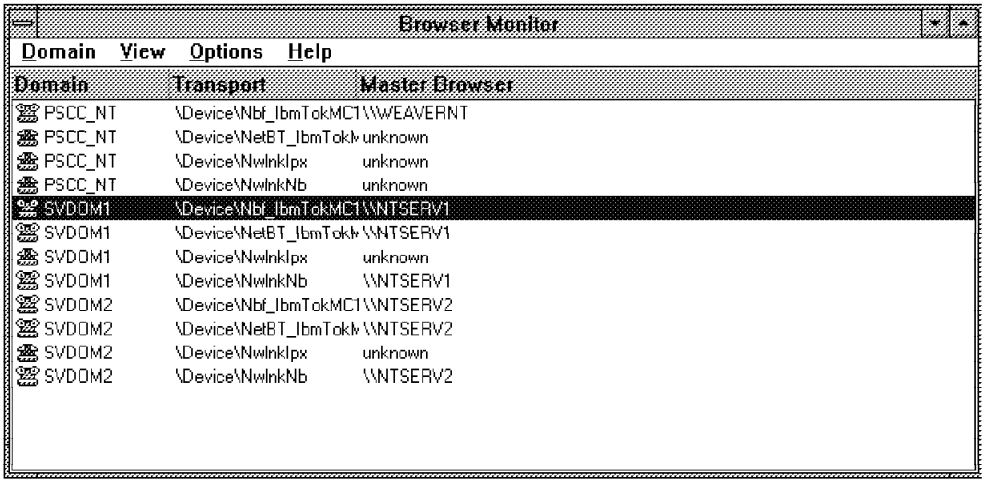


Figure 114. Browser Monitor

To add other domains, choose **Domain** from the top menu and then **Add Domain**. Insert the domain name or select the domain from the list. There will be an entry for all locally defined network transport protocols. To delete entries you don't need select the item and press delete.

To get detailed information about the shown master browser, double-click on its line to view the properties. The status of servers and domains for the browser service are shown below:

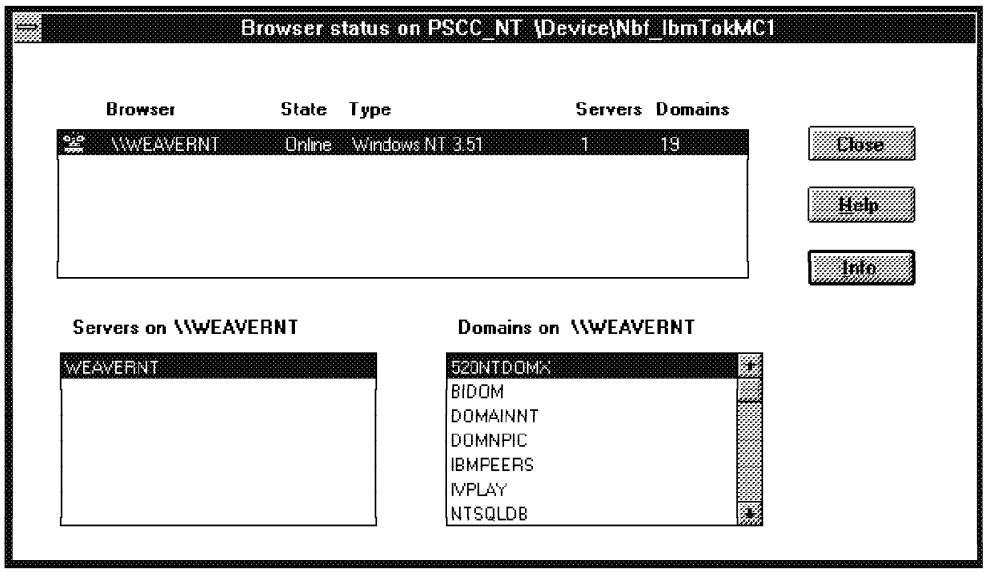


Figure 115. Browser Monitor - Browser Status

By clicking on the **Info** button, a window with the browsers statistics is shown.

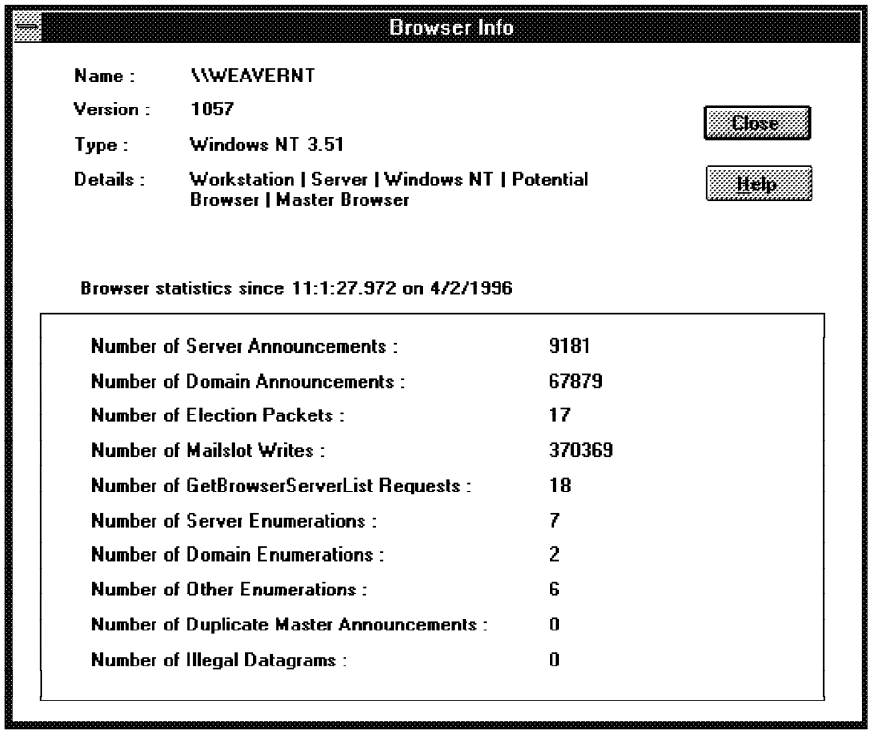

Browser Info
Name :
\\WEAVERNT
Version :
1057
Type :
Windows NT 3.51
Details :
Workstation | Server | Windows NT | Potential Browser | Master Browser
Close
Help
Browser statistics since 11:1:27.972 on 4/2/1996
Number of Server Announcements : 9181
Number of Domain Announcements : 67879
Number of Election Packets : 17
Number of Mailslot Writes : 370369
Number of GetBrowserServerList Requests : 18
Number of Server Enumerations : 7
Number of Domain Enumerations : 2
Number of Other Enumerations : 6
Number of Duplicate Master Announcements : 0
Number of Illegal Datagrams : 0

Figure 116. Browser Monitor - Browser Statistics

Select the refresh rate for Browser Monitor by choosing **Options** and **Intervals**. Enter a value in seconds. (Default is 900 seconds.) Do not choose too short of a value because every check causes quite a lot of network traffic.

2.3.5.3 Domain Monitor

With the Domain Monitor (DOMMON.EXE) you can supervise multiple domains and the status of the Domain Controller Service and the trusted domains.

To do so do the following:

1. Open the **Domain Monitor**.
2. Add one or more domain by choosing **Domain** and **Add Domain**.

The status of the domains will be shown with graphical indicators:

- A green domain sign indicates that the domain controller is found, is working and all connections are established.
- A red domain sign indicates that the domain controller is found but one or more connections could not be established.
- A crossed out red domain sign indicates that the domain controller could not be found and therefore no connections could be made.

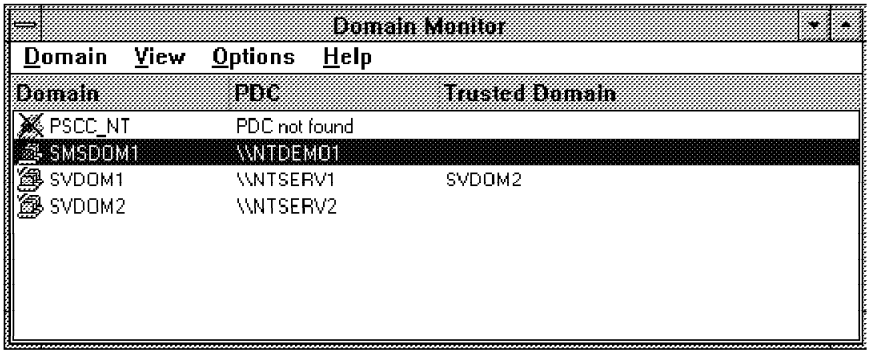


Figure 117. Domain Monitor

The Domain Monitor shows also the domain trusts and, if the option Monitor Trusted Domain is selected, they can also be monitored.

By double-clicking on the desired domain, the domain properties are shown. It provides information about the subservices of the domain controller service. Select a trusted domain controller and double-click for more information about the server.

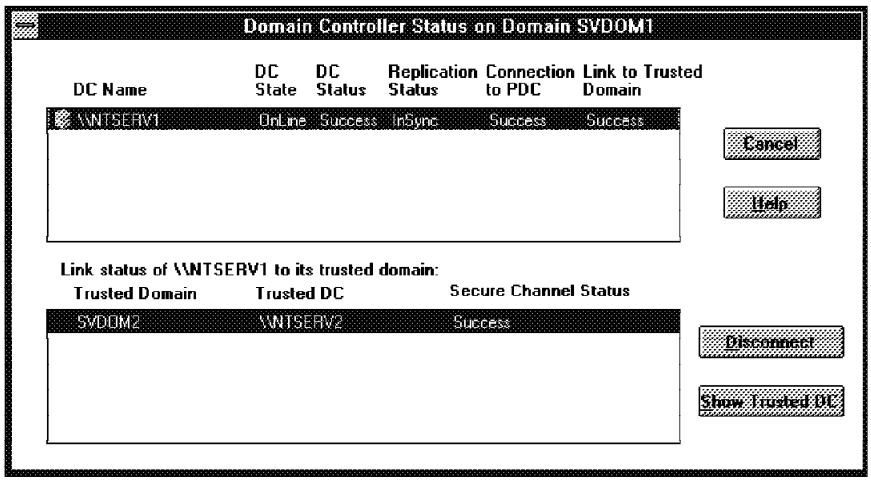


Figure 118. Domain Monitor - Domain Controller Status

Windows NT Domain Monitor can not be used on IBM LAN Server Domains or on any workgroups; use it only with Windows NT Server Domains.

2.3.6 Windows NT Setup Manager

Windows NT Setup Manager (SETUPMGR.EXE) is a tool to create answer files for unattended or predefined installation of Windows NT.

The answer file contains answer values for the input to be provided during the setup process. This makes it possible to install a system unattended or with little user interaction. There can be either an individual answer file for each computer you want to install or one file for multiple computers if they're installed the same way.

Start WINNT or WINNT32 with this answer file specified in the following way:

```
WINNT /u:ANSWER FILE          (for 16-bit setup version)
or
WINNT32 /u:ANSWER FILE        (for 32-bit setup version)
```

To create a setup answer file with the Setup Manager do the following:

1. Start the **SETUPMGR.EXE** program. The Windows NT Setup Manager dialog appears.
2. If you want to edit an existing unattended answer file, click on the **Open** button and open the desired file.
3. Specify the settings according to the system to be installed.

   Note: The configuration data you have to provide depends on the role of the new Windows NT installation. Also note that you have to define whether it is going to be a new installation or an update from either Windows 3.x or an older Windows NT version.
4. Specify the file name you want to save the script file as.
5. Choose **OK** to close Setup Manager.

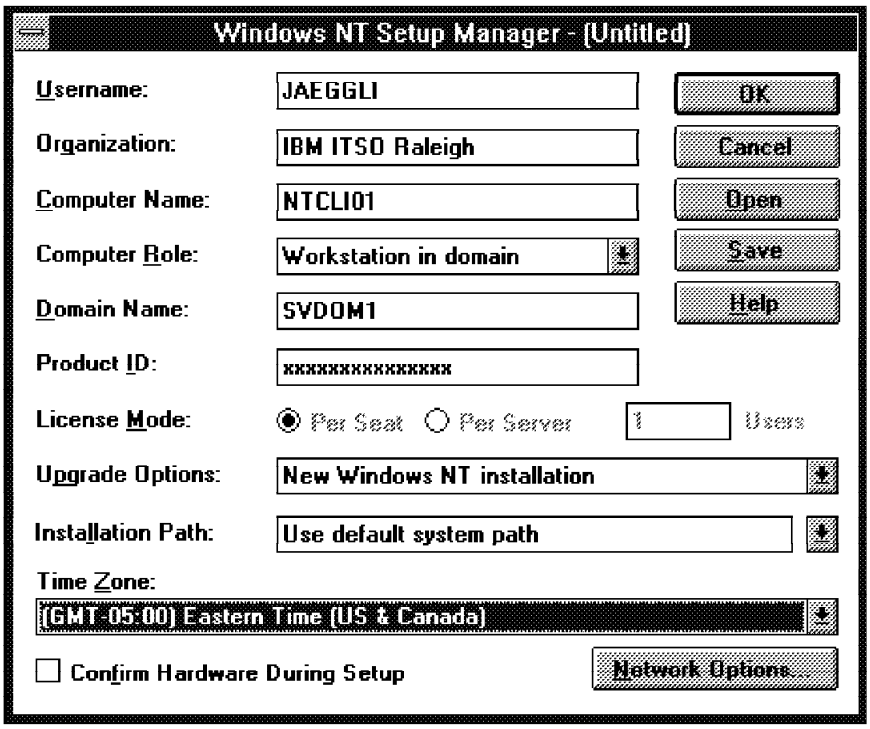


Figure 119. Windows NT Setup Manager (SETUPMGR.EXE)

By clicking on **Network Options** you can define the network transport protocol the system should use and select an adapter card. Usually it's best to let the system autodetect the card.

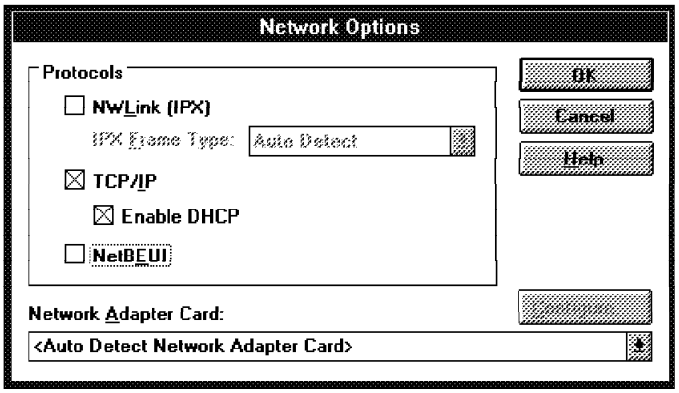


Figure 120. Windows NT Setup Manager - Network Options

Note

You can not define an IP address for a specific system in the Setup Manager. If your system does not use DHCP Service, you have to set up the information in the file %systemroot%\system32\IPINFO.INF. Each target machine will require a unique IP address in the IPINFO.INF file. Read the header of this file for more instructions.

If any information needed by the setup process is omitted, the setup program will prompt the user to provide this information. A copy of the comments from the IPINFO.INF file is shown below:

```
; Copyright (C) 1993 Microsoft Corporation
; All rights reserved.
;
; The ipinfo.inf file allows network administrators to provide smart
; defaults for TCP/IP configuration parameters. By modifying this
; template, an administrator can distribute the Windows NT TCP/IP
; software over the network or on floppy disks to users with some
; smart default configuration parameters. End users will still be
; able to modify these values when installing TCP/IP, however, the
; default values will be automatically filled in for them.
;
; This file may contain defaults for the default gateway, IP
; addresses (per interface), and subnet mask (per interface). To modify
; the default 'default gateway' edit the line in the ·DefaultIPInfo"
; section below that looks like this:
;       DefaultGateway = "xxx.xxx.xxx.xxx"
;
; xxx.xxx.xxx.xxx represents a valid IP address for the default
; gateway. If the default gateway is unknown, it can be left blank:
;
;       DefaultGateway = ""
;
; To modify the default IP addresses and subnet mask IP addresses,
; modify the following lines in the ·DefaultIPInfo" section below:
;       NumberOfIPAddress = X
;
; X represents the number of IP addresses for the machine.
;
; Add the following pair of values for each interface <X>:
;       IPAddress<Y>  = "xxx.xxx.xxx.xxx"
;       SubnetMask<Y> = "xxx.xxx.xxx.xxx"
;
; where 1 <= Y <=X and <Y> represents the interface(s) on the system.
; The IPAddress and SubnetMask values can be left blank ("") for no
; default, or can be set with valid IP addresses.
;
; For example:
;·DefaultIPInfo"
;    DefaultGateway = "11.1.0.0"
;    NumberOfIPAddress = 3
;    IPAddress1  = "11.1.12.1"
;    SubnetMask1 = "255.255.0.1"
;    IPAddress2  = "11.1.12.2"
;    SubnetMask2 = "255.255.0.2"
;    IPAddress3  = "11.1.12.3"
;    SubnetMask3 = "255.255.0.3"
;------------------------------------------------------------------------
; GetIPInfo: Returns the default gateway IP address, a list of default IP
;       addresses and a list of default subnet mask IP addresses to the
;       caller.
```

2.3.6.1 NT Registry Guide

The NT Resource Kit also includes detailed help on the fields that are located in the NT registry. An outline of that is shown below:

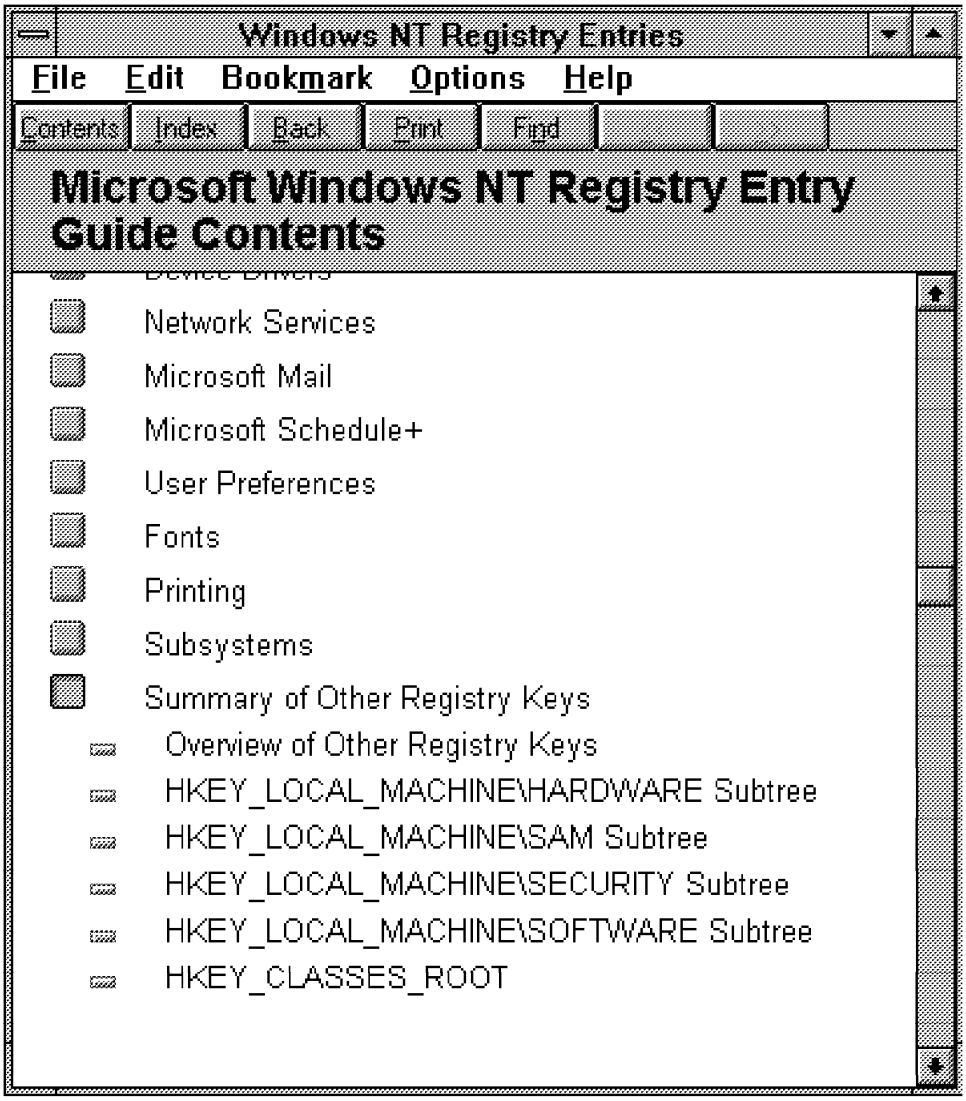


Figure 121. NT Registry Contents

Chapter 3. Alert Flows

This chapter covers alert generation and alert forwarding within Windows NT by looking at two different methods:

- Alerts generated by TME 10 NetFinity
- Alerts generated by Windows NT Performance Monitor

3.1 Alerts by TME 10 NetFinity

Within TME 10 NetFinity, multiple services have the capability to generate alerts and forward them to the TME 10 NetFinity Alert Manager. Every service acts as an agent on the supervised system and generates the alert depending on the alert condition configuration. The Alert Manager collects the alerts and handles them according to the alert profiles.

3.1.1 Alert Manager

The Alert Manager receives and collects the alerts from different TME 10 NetFinity Services running on the local or remote systems. Depending in the defined actions, the alerts are forwarded, displayed or logged to the system logs.

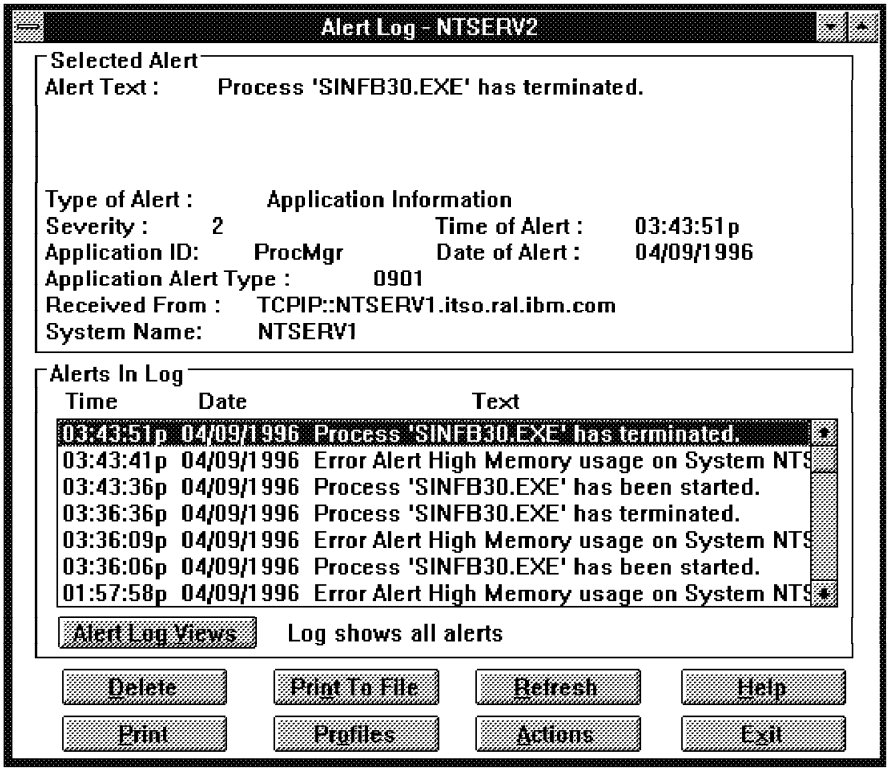

Alert Log - NTSERV2
Selected Alert
Alert Text : Process 'SINFB30.EXE' has terminated.
Type of Alert : Application Information
Severity : 2
Time of Alert : 03:43:51p
Application ID: ProcMgr
Date of Alert : 04/09/1996
Application Alert Type : 0901
Received From : TCPIP::NTSERV1.itso.ral.ibm.com
System Name: NTSERV1
Alerts In Log
Time Date Text
03:43:51p 04/09/1996 Process 'SINFB30.EXE' has terminated.
03:43:41p 04/09/1996 Error Alert High Memory usage on System NT
03:43:36p 04/09/1996 Process 'SINFB30.EXE' has been started.
03:36:36p 04/09/1996 Process 'SINFB30.EXE' has terminated.
03:36:09p 04/09/1996 Error Alert High Memory usage on System NT
03:36:06p 04/09/1996 Process 'SINFB30.EXE' has been started.
01:57:58p 04/09/1996 Error Alert High Memory usage on System NT
Alert Log Views
Log shows all alerts
Delete
Print To File
Refresh
Help
Print
Profiles
Actions
Exit

Figure 122. Alert Manager

The Alert Manager lets you see the received alerts, browse through the alert log, delete alerts, print alerts to printer or to a file.

For defining profiles refer to 3.2.2, “Alert Profiles” on page 99.

For defining actions refer to 3.2.4, “Alert Actions” on page 100.

© Copyright IBM Corp. 1996

If you click on Alert Log Views, you can set a filter to the alert log, depending on predefined profiles.

3.2 View Alert Log

To view the alert log, simply click on the alert and the alert details are displayed in the upper half of the window.

To set a filter to see only specific alarms do the following:

1. Click on **Alert Log Views**.
2. Set time and date range if desired.
3. Activate one or more profiles.
4. Check the **Enable** box for the time and date range and/or the active profiles.
5. Click on **Refresh** to filter the alarm log.

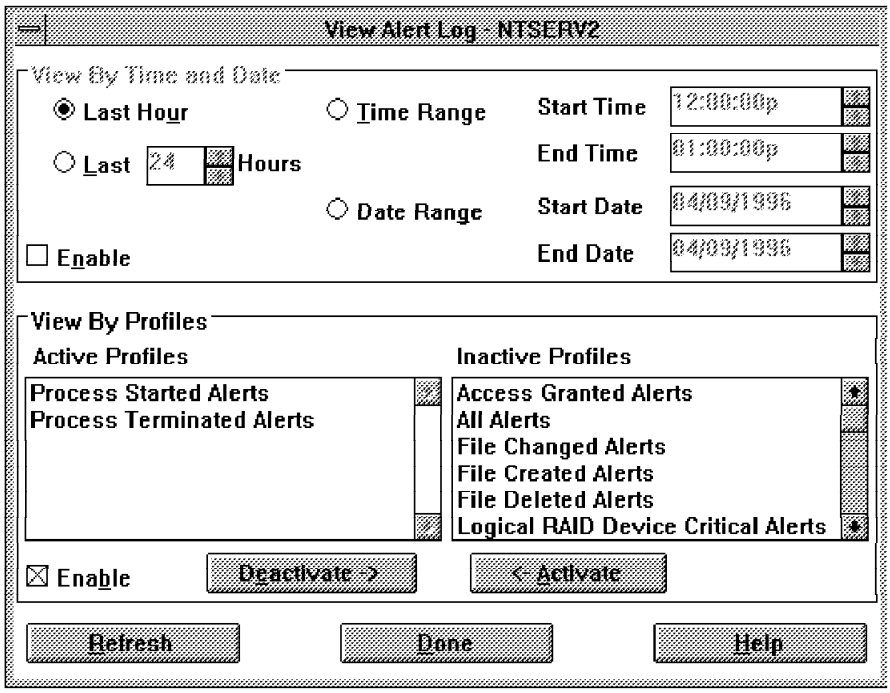


Figure 123. Alert Manager - Set Filter to Alert Log

3.2.1 Alert Forwarding and Alert Flow

From the Alert Manager, alerts can be sent to many different destinations.

Figure 124 on page 97 shows a possible configuration for corporate-wide alert management with TME 10 NetFinity.

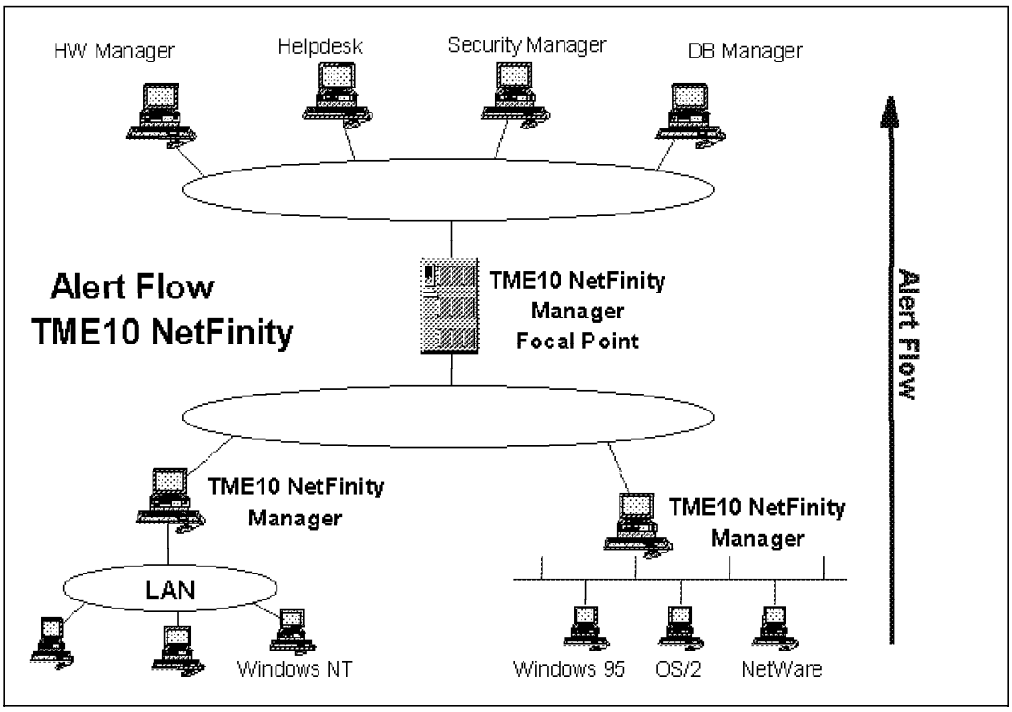


Figure 124. Alert Flow in a Corporate Environment

- From each local network the workstations and servers report all their alerts to the Alert Manager of the local TME 10 NetFinity Manager.
- The local Alert Manager forwards the alerts to the focal point Alert Manager.
- The focal point Alert Manager writes the alerts to its log file and resends the alerts according to the alert type and severity to the alert manager on the workstation of the responsible person.

This alert forwarding can involve different operating systems for clients and managers and also use multiple network protocols. For example, a Novell Server reports a RAID error to the local manager running on Windows NT over IPX. This forwards the error alert over the WAN through TCP/IP to the focal point manager running on OS/2. From here the alert goes on an SNA link to the host system and to the hardware administrator's terminal.

This is only one of the ways of how an alert flow can be defined. It is also possible to involve more hierarchy stages or route alerts to multiple systems.

Alert forwarding is defined from the action button in the Alert Manager. It can be defined in two ways:

- By alert conditions
- By profiles

3.2.1.1 Defining Alert Forwarding by Alert Conditions

To define alerts that can be forwarded by other systems do the following:

1. Open the **Alert Manager**.
2. Click on **Action**.
3. Click on **New** to add a new forwarding action.
4. Choose **Bind to...** from the top menu and select **Alert Conditions**.

5. Select one or more

Alert Type	Depends on the application ID
Severity	See 3.2.3, “Severity” on page 100
Application ID	See 3.2.6, “Applications Sending Alerts to the Alert Manager” on page 104
Application Alert Type	Depends on the application ID
Sender	To receive alerts from remote systems

6. Define an action to be taken if the alert responds to the above definitions (see 3.2.4, “Alert Actions” on page 100).
7. Click on **Save** to save the new action.

An example of an alert filter follows:

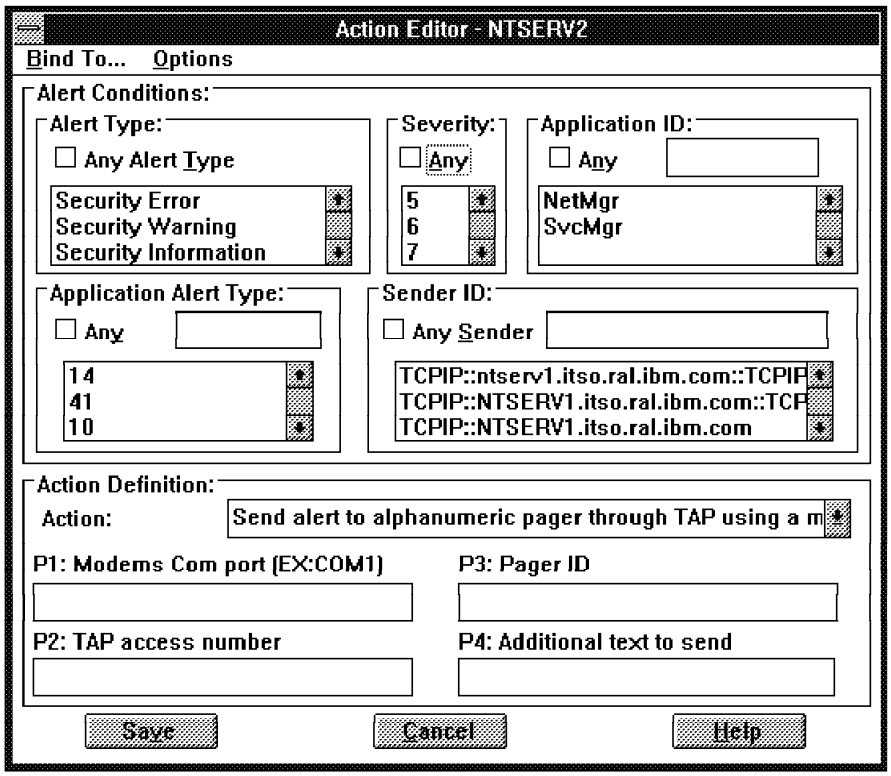


Figure 125. Alert Manager - Action Editor

3.2.1.2 Defining Alert Forwarding by Profiles

1. Open the **Alert Manager**.
2. Click on **Action**.
3. Click on **New** to add a new forwarding action.
4. Choose **Bind to...** from the top menu and select **Profiles**.
5. Select one or more profiles from the right window and click on **Trigger by** to select the profiles.
6. Enter a name for this action in the field Action Label.
7. Click on **Save** to save the new action.

8. Define an action to be taken if the alert responds to the above profiles (see 3.2.2, “Alert Profiles” on page 99).

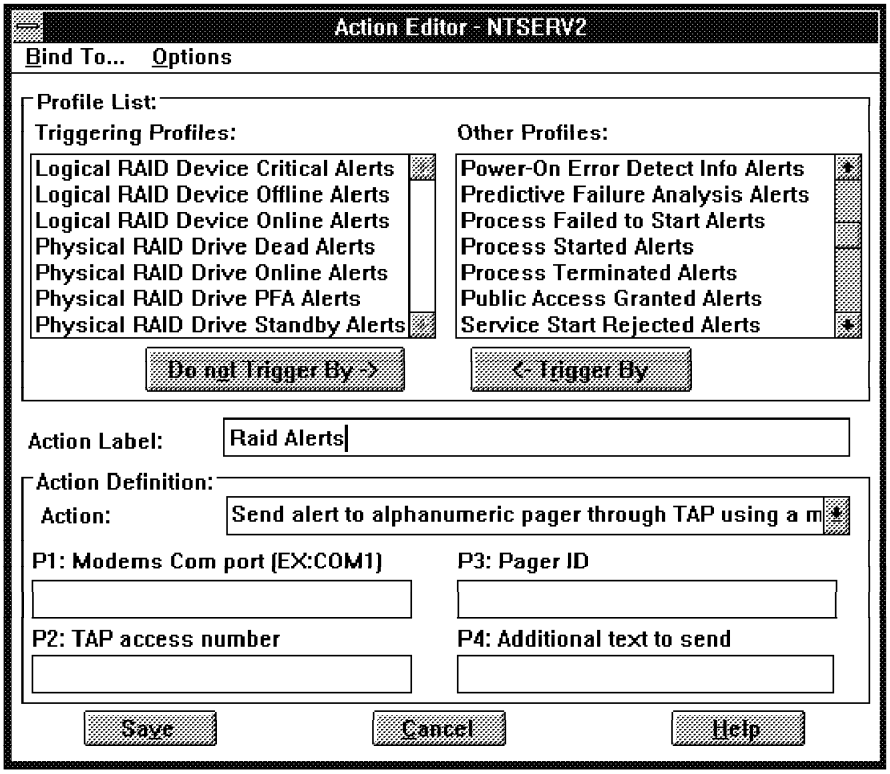


Figure 126. Alert Manager - Action Editor

3.2.2 Alert Profiles

Alert profiles are objects that help the user better manage the alerts received by the system. In TME 10 NetFinity many alert profiles are predefined. Open the Profile Editor by clicking on **Profiles** and browse through the profiles. If you do not find the profile that exactly matches your needs, you can either create a new profile or change an existing one.

There are two possibilities to define a profile:

- By alert conditions
- By other profiles

To define a profile by alert conditions is the same as defining an alert by alert condition (see 3.2.1.1, “Defining Alert Forwarding by Alert Conditions” on page 97).

To define a profile by other profiles:

1. Open the **Alert Manager**.
2. Click on **Profiles**.
3. Click on **New** to add a new profile.
4. Choose **Define By...** from the top menu and select **Profile Composition**.
5. Select one or more profile from the right window and click on **Include** to select the profiles.

6. Enter a name for the new profile in the field Profile Name.
7. Click on **Save** to save the new profile.

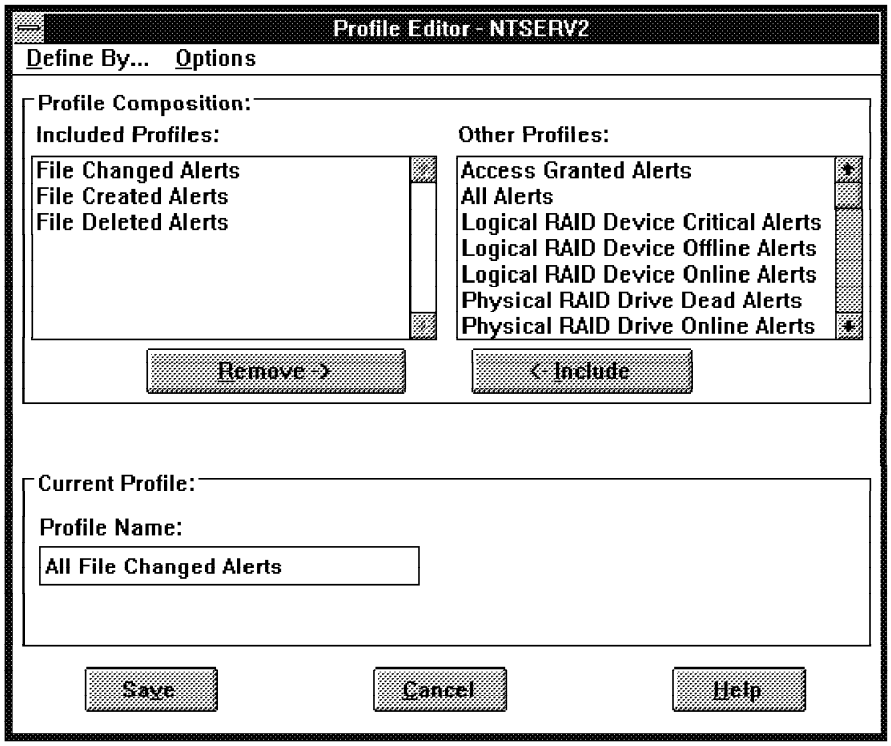


Figure 127. Alert Manager - Edit Profiles by Profile Composition

3.2.3 Severity

The severity code classifies the importance of an alert. The range is from 0 (Failure) to 7 (Information). The lower the importance of an error the higher the severity code value. That means a severity code of 0 is very important and immediate action should be taken as response to the alert. The severity code 7 is used for information and no action has to be taken.

The severity code is one of the alert attributes used to classify and filter alert messages. This attribute is also used to define forwarding profiles.

3.2.4 Alert Actions

The following actions can be defined for alert forwarding in the Alert Editor window of the Alert Manager:

- Send alert to alphanumeric pager through TAP using a modem

  Forward the alarm to a alphanumeric pager through the Telephone Application Program (TAP). Define the COM Port (P1) where the modem is connected and enter the pager's ID (P3), the TAP access number (P2) and additional text (P4) to be sent to the pager.

- Activate a numeric pager using a modem

  Forward the alarm to a numeric pager. Define the COM port where the modem is connected and enter the pager's telephone number.

- Notify user with pop-up

The Alert Received window will pop up and display the alarm to the user logged in to the system.

- Execute command '<P1>'

  On every occurrence of the defined alarm condition, the command '<P1>' will be executed in foreground. Include drive, path and parameters in the command statement.

  The following variables can be passed with the command line as parameters to the command. They are provided from the alert manager and contain alert specific data.

%TXT	Alert text
%TIM	Alert time
%DAT	Alert date
%SEV	Alert severity
%SND	Alert sender (for example, TCPIP::NTSERV2.ITSO.RAL.IBM.COM)
%TYP	Alert type
%APP	Alert application ID
%AT	Alert application-specific type
%P1 - %P9	Alert-specific text strings. The availability and the contents of these parameters depend on the alert. See *TME 10 NetFinity Manager, User's Guide*, Appendix I, for more information.

- Execute minimized command '<P1>'

  On every occurrence of the defined alarm condition, the command '<P1>' will be executed in the background icon. Include Drive, Path and Parameters in the command statement.

  Same parameter variables as for **Execute command '<P1>'** applied.

- Set error condition '<P1>' for sending system

  This sets the circle and stripe sign over the icon of the system in the Remote System Manager Group window if this alert from this system is received. The '<P1>' error condition is shown if opening the Error Conditions of the system properties (right mouse button on the system icon) in the Remote System Manager

- Clear error condition '<P1>' for sending system

  This removes the circle and stripe sign from the icon of the system in the Remote System Manager Group window if this alert from this system is received.

- Add Event to Event Log

  The Alert Message is written to the Windows NT Application Log and can be viewed with the Event Viewer.

- Send to E-Mail via MAPI interface

  The Alert Manager creates an E-Mail with the alert message and sends it using the Microsoft Windows Mail Application Programming Interface (MAPI), for example, via MS Mail or Exchange. Enter Password (P1) and User ID (P3)

of a defined mail user and the E-Mail address of the receiver (P2) into the appropriate fields.

- Add alert to log file

  Writes the alert to the log file of the Alert Manager.

- Export to a DB2 Database

  This action is only available if the data export to DB2 is defined. It will append a database record for each alert.

- Export Database Information via ODBC

  This action is only available if the data export through the ODBC interface is defined. It will append a database record for each alert.

- Forward alert through network <P1> to system <P2>

  The alert will be forwarded to another Alert Manager through the network. <P1> stands for one of the network driver configuration enabled network protocols (TCP/IP, NetBIOS, IPX). <P2> stands for the network name of the receiver and depends on the protocol.

- Play waveform file '<P1>'

  If your system is equipped for sound, the waveform file '<P1>' will be played on alert.

- Send SNMP Alert

  Sends an SNMP alert to other systems according the SNMP configuration in the Windows NT network support.

3.2.5 Command Line Interface

With the GENALERT.EXE command you can also define your own TME 10 NetFinity alert (see Figure 128 on page 103 for command line syntax). This command can be issued from a batch file or from other programs as an external command.

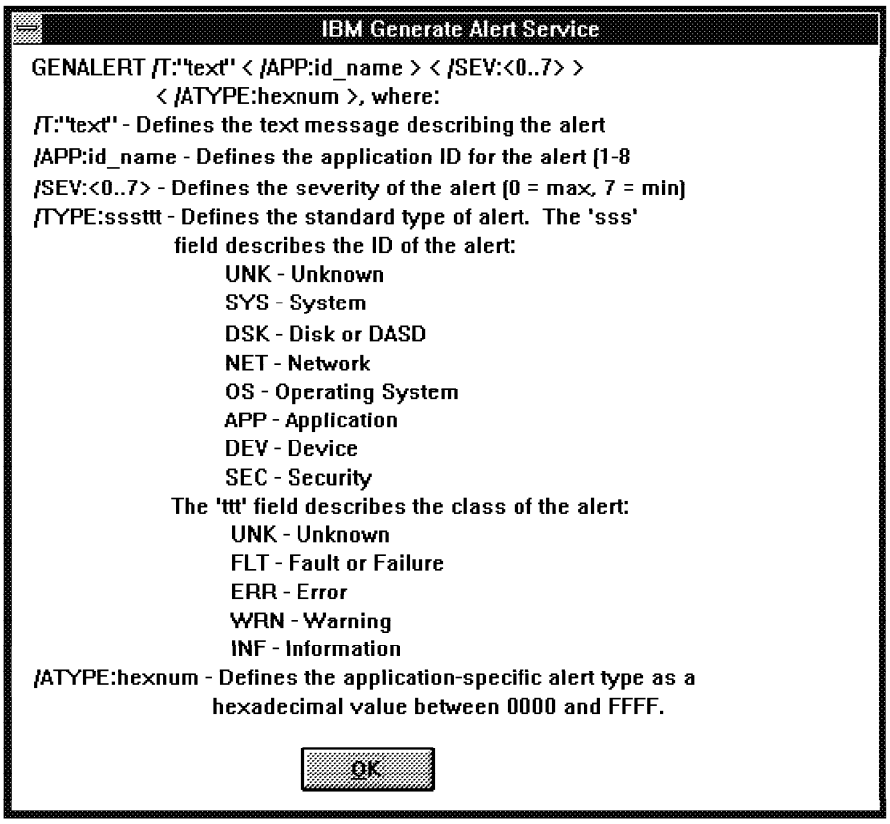

IBM Generate Alert Service
GENALERT /T:"text" < /APP:id_name > < /SEV:<0..7> >
< /ATYPE:hexnum >, where:
/T:"text" - Defines the text message describing the alert
/APP:id_name - Defines the application ID for the alert (1-8
/SEV:<0..7> - Defines the severity of the alert (0 = max, 7 = min)
/TYPE:sssttt - Defines the standard type of alert. The 'sss'
field describes the ID of the alert:
UNK - Unknown
SYS - System
DSK - Disk or DASD
NET - Network
OS - Operating System
APP - Application
DEV - Device
SEC - Security
The 'ttt' field describes the class of the alert:
UNK - Unknown
FLT - Fault or Failure
ERR - Error
WRN - Warning
INF - Information
/ATYPE:hexnum - Defines the application-specific alert type as a
hexadecimal value between 0000 and FFFF.
OK

Figure 128. GENALERT.EXE - Command Line Syntax

An example of a genalert and its resulting alert follows:

```
genalert /t:"Genalert test" /sev:3 /atype:0001 /APP:user /type:appinf /atype:55
```

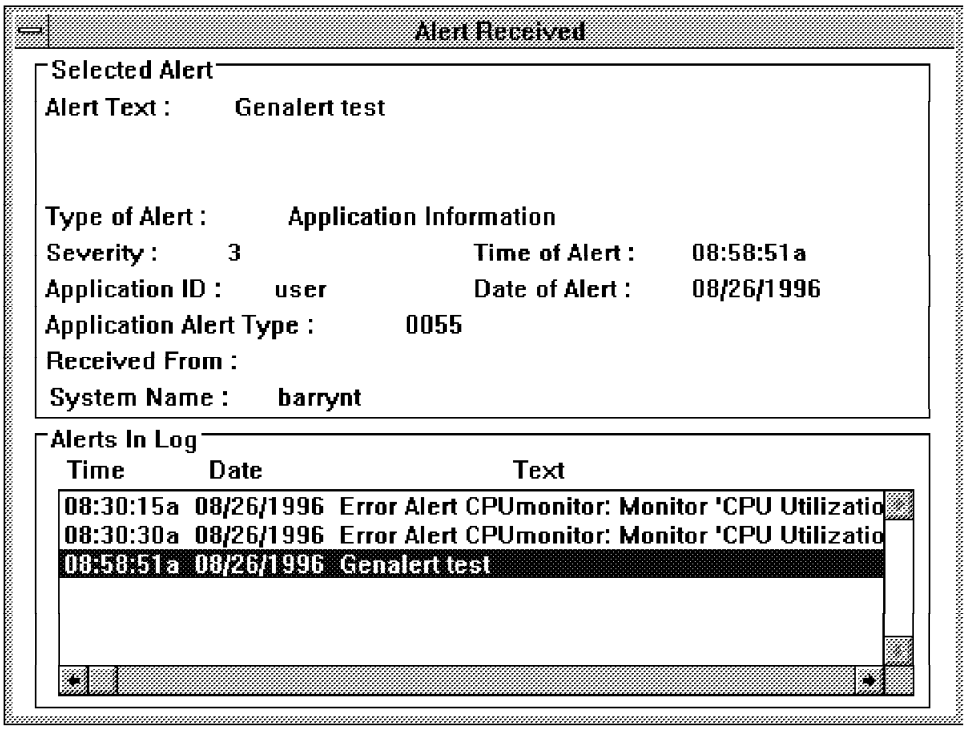

Alert Received
Selected Alert
Alert Text : Genalert test
Type of Alert : Application Information
Severity : 3
Time of Alert : 08:58:51a
Application ID : user
Date of Alert : 08/26/1996
Application Alert Type : 0055
Received From :
System Name : barrynt
Alerts In Log
Time Date Text
08:30:15a 08/26/1996 Error Alert CPUmonitor: Monitor 'CPU Utilizatio
08:30:30a 08/26/1996 Error Alert CPUmonitor: Monitor 'CPU Utilizatio
08:58:51a 08/26/1996 Genalert test

Figure 129. Generated Alert

3.2.6 Applications Sending Alerts to the Alert Manager

For detailed information about the TME 10 NetFinity functions mentioned here, please see 2.1.1, " TME 10 NetFinity Functions for Services" on page 12. In this paragraph only the alert handling is described.

Note

Most of the following definitions can be ether done from the administered system itself or remotely through the Remote System Manager. However, all guidelines given here, refer to the managed system.

3.2.6.1 Security Manager

The Security Manager will create an alert if access for a TME 10 NetFinity service is granted or rejected to a user or another service. This depends on the profile defined for the user. Please refer to 2.1.1, " TME 10 NetFinity Functions for Services" on page 12 for how to define the user profile.

By default, all access rights are granted to the user public, which means that everybody has all rights.

To define alert conditions:

1. Start the **Security Manager**.
2. Choose **Edit/Display Incoming Passwords**.
3. Create one or more new user profiles and save them.
4. Remove all access rights from the user public including the Security Manager Access. (You can not remove the user itself.)
5. Click on **Set** to activate the new profiles.
6. Click on **Exit** to leave the Security Manager.

If you make a mistake and remove the access rights for public before adding the new user IDs, you can always delete the SEC.INI file. It will reset the password profile back to the default of just public.

For every attempt to connect to the TME 10 NetFinity Services remotely, an alert will be generated. Another alert will be initiated whether the access is granted or denied.

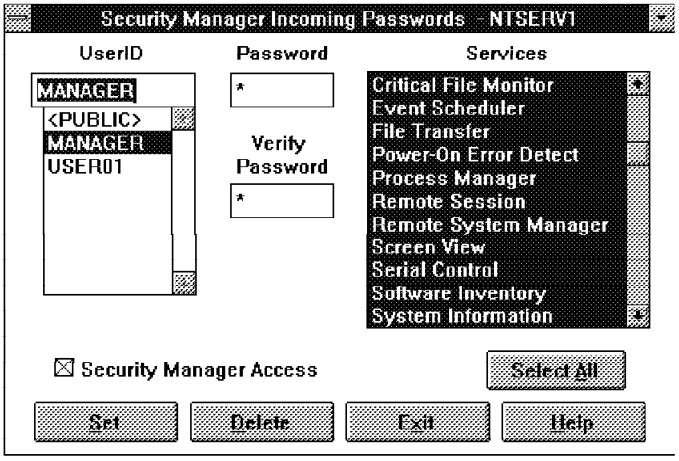


Figure 130. Security Manager - User Profile Definition

Note

In the version we were testing, alerts with a severity code 6 or 7 were not forwarded to other systems nor written to the system log. They were only displayed in the alert log.

3.2.6.2 System Monitor

The System Monitor shows you the usage of a variety of system resources on the managed system. The monitors that are available are dependent upon the operating system (for example, NT may have some monitors that OS/2 doesn't have), and the characteristics of the system. For example, if you have TCP/IP, you will be able to monitor TCP/IP metrics. For all of these resources, thresholds for minimums and maximums can be set. If the actual value exceeds these thresholds an alarm is generated.

To define thresholds:

1. Start the **System Monitor Service**.
2. Choose **Windows**, **Show Monitors** and highlight the monitors to select them for display.

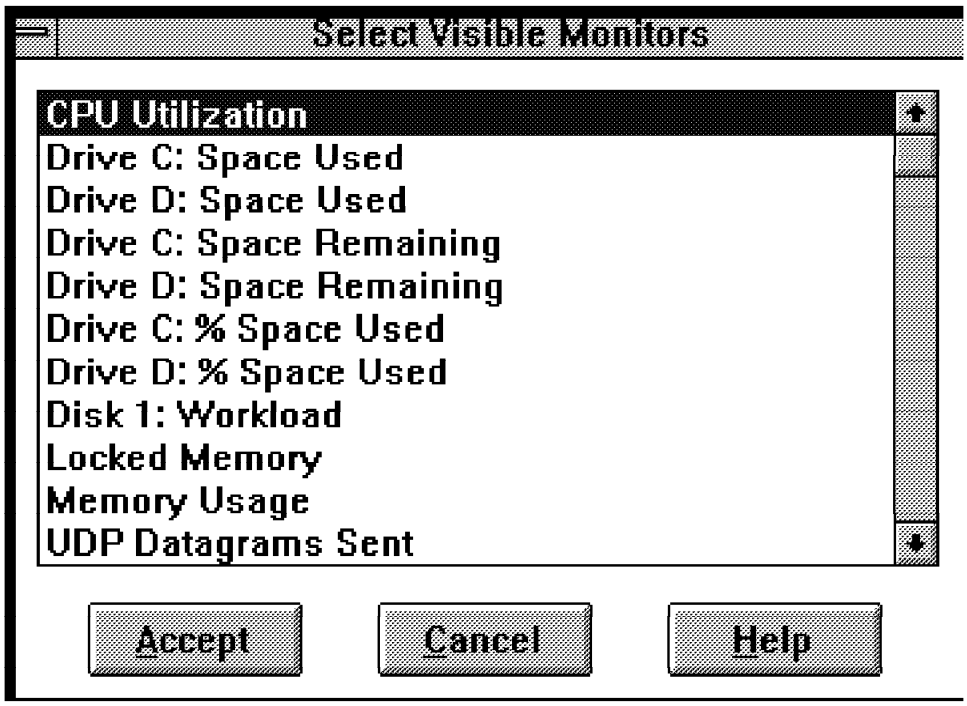


Figure 131. Visible Monitors

3. To define a threshold value, click with the right mouse button on the desired monitor.
4. Choose **Open** and **Threshold** to display the threshold definitions.
5. Enter a name for the threshold and press Enter.

   You must press Enter as tabbing or selecting another field won't do the job.
6. Define the value and severity for one or more alert conditions:
   - Error if above or equal to *value* with *severity*.
   - Warning if above or equal to *value* with *severity*.
   - Alert on return to normal with *severity*.
   - Warning if below or equal to *value* with *severity*.
   - Error if below or equal to *value* with *severity*.

   Do not forget to check the **Notify** box for every defined alert condition.
7. Set the duration interval value to be higher or lower then the threshold before the alert is generated.
8. Set a value for the Resend Delay field if the alert should be resent while the actual value stays above or below the threshold.

   If you want the alert to be sent only once, set the Resend Delay to never.
9. Finally, click on **Create** to save the threshold definition.
10. Close the window.

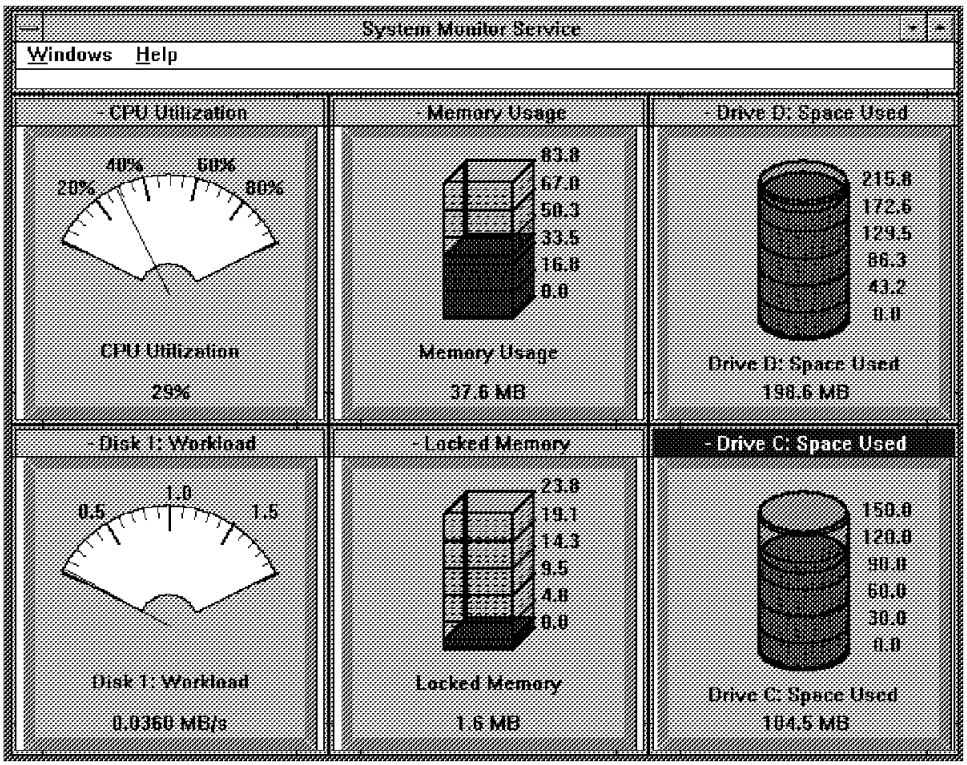


Figure 132. System Monitor Service - System Monitors

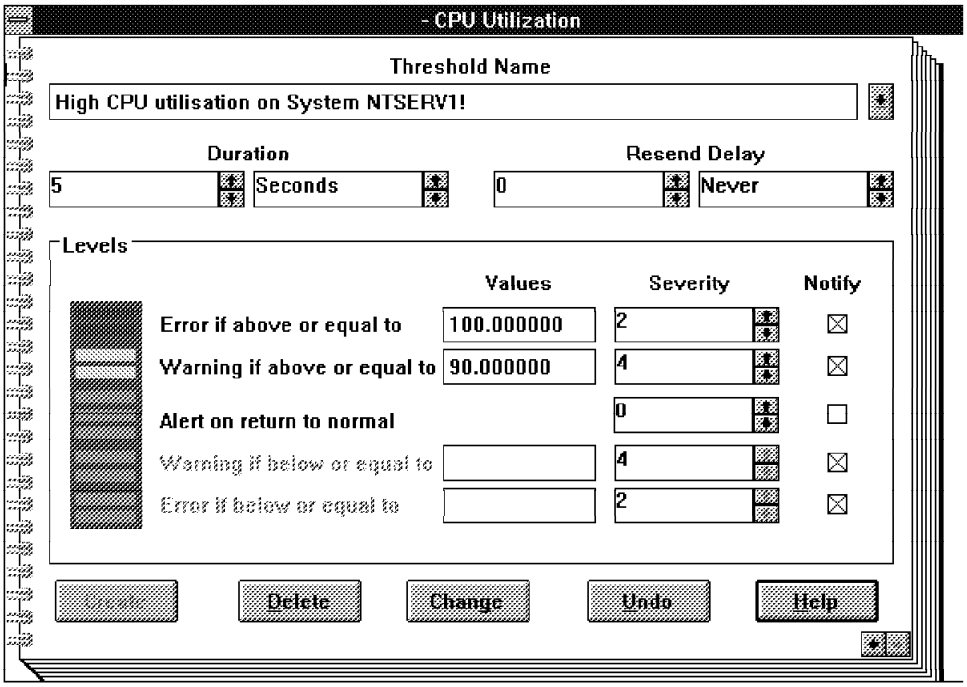


Figure 133. System Monitor Service - Threshold Definition

3.2.6.3 Power-On Error Detect

The Power-On Error Detect (POED) utility listens to the network segment for systems reporting errors while executing the power-on self test (POST). Systems with system partition can be enabled to report POST errors through the network. They will send a broadcast package to all systems running the POED service.

If you have a central systems manager to control all workstations in a multiple segment network, you need at least one system running the POED service per segment to forward the alert to the central manager.

To set up alerting:

1. Install the POED Utility Disk on the System Partition of the managed systems.
2. Start the POED interface on the TME 10 NetFinity Manager.
3. Choose **Options**.
4. Make sure Alert on Error has a check mark.
5. Choose **File** and **Exit** to leave the program.

Now all POED incidents will create an entry in the alert manager log and the alerts can be forwarded through the alert manager.

3.2.6.4 Predictive Failure Analysis

Predictive Failure Analysis (PFA) can warn you if a disk has a hardware problem or will probably encounter a major hardware problem. PFA is only supported for PFA-enabled disk drives.

To define an alert condition do the following:

1. Start the **PFA Service**.
2. Double-click on the icon of the disk you would like to supervise.
3. See Text for alert message for the text that will be sent with the alert and enter additional text to be sent.
4. Check the **Generate Alert** box and select a severity class.
5. Click on **Exit** to add set the alert condition.

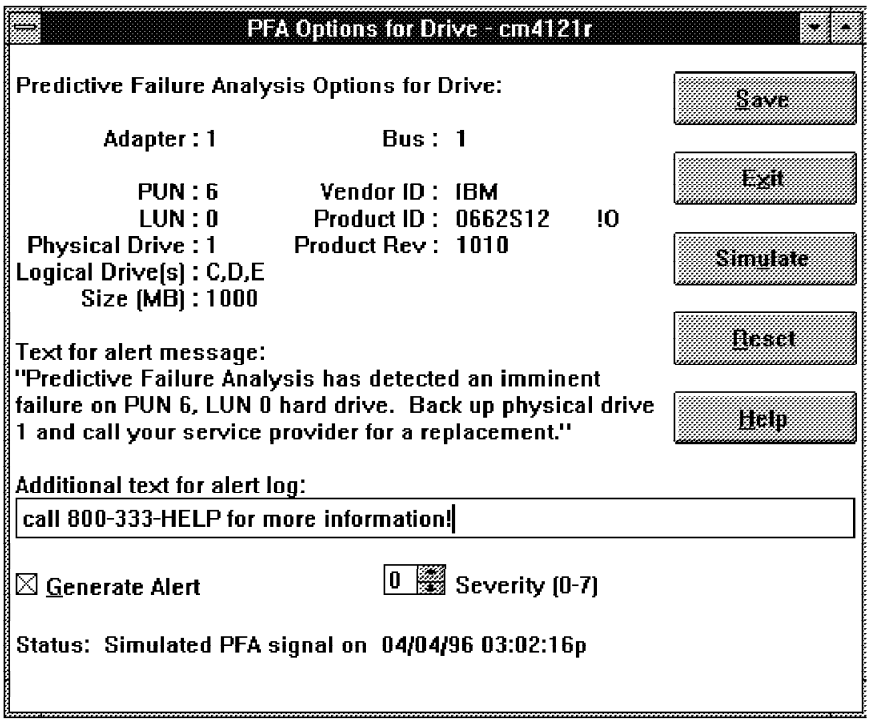

PFA Options for Drive - cm4121r
Predictive Failure Analysis Options for Drive:
Adapter : 1
Bus : 1
PUN : 6
LUN : 0
Physical Drive : 1
Logical Drive(s) : C,D,E
Size (MB) : 1000
Vendor ID : IBM
Product ID : 0662S12
Product Rev : 1010
!O
Save
Exit
Simulate
Reset
Help
Text for alert message:
"Predictive Failure Analysis has detected an imminent failure on PUN 6, LUN 0 hard drive. Back up physical drive 1 and call your service provider for a replacement."
Additional text for alert log:
call 800-333-HELP for more information!
Generate Alert
0
Severity (0-7)
Status: Simulated PFA signal on 04/04/96 03:02:16p

Figure 134. Predictive Failure Analysis - PFA Options

3.2.6.5 Critical File Monitor

The Critical File Monitor supervises system files or other files defined by users and sends an alert to the Alert Manager if one of these files are changed, deleted or created.

To define an alert condition do the following:

1. Start the **Critical File Monitor**.
2. Check the boxes for the **System Files** and select a severity class if you want these files supervised.
3. Click on **(monitor another file)** to add additional files to supervise.
4. Enter the file name or browse and select the file.
5. Select a severity class.
6. Click on **Monitor** to add this file to the supervised files.

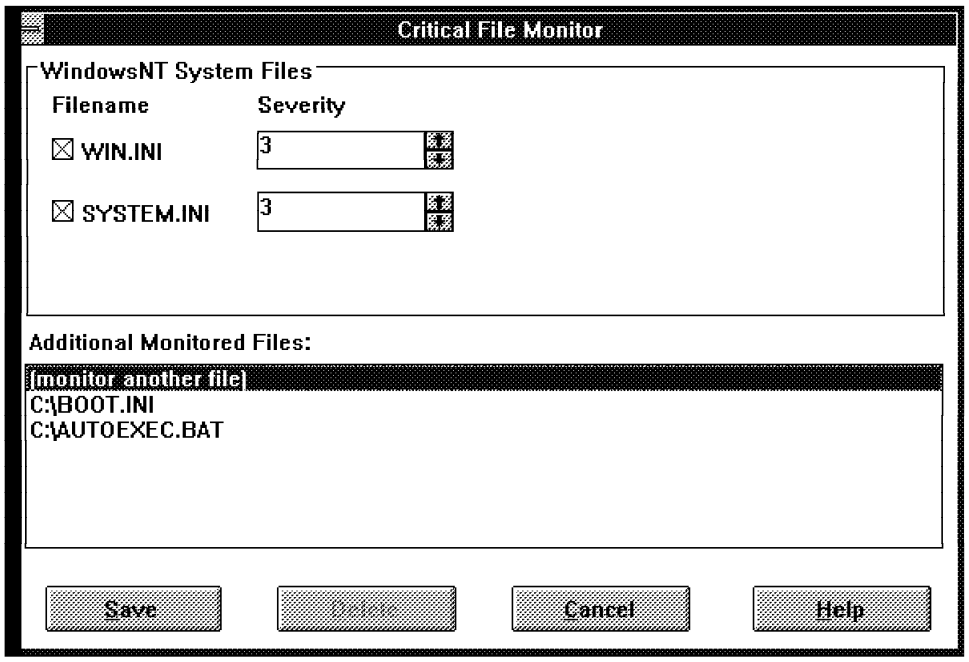


Figure 135. Critical File Monitor - System Files

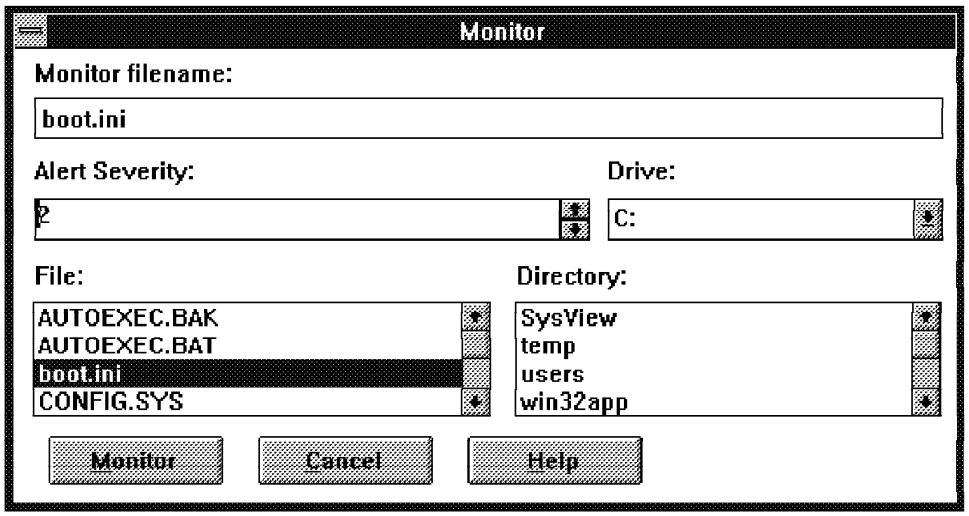


Figure 136. Critical File Monitor - Monitor Additional File

3.2.6.6 Process Manager

The Process Manager controls the active System Processes of Windows NT. For every process, an alert can be generated if the process starts, stops or is not running.

To define an alert condition do the following:

1. Start the **Process Manager**.
2. Choose **Process** and **Process Alerts**.
3. Click on **Add** to add a new alert condition.

4. Enter the program execution file name in the field Program, including the file extension.
5. Select the severity class.
6. Select one or more alert conditions.

   For the Generate alert if program not started field, define a time-out after the program must be active, otherwise the alert is not generated.
7. Check the **Notify** box.

   If the Notify box is not checked, no alert will be generated. This is useful if you want a defined alert temporarily to disable.
8. Click on **OK** to set the condition.

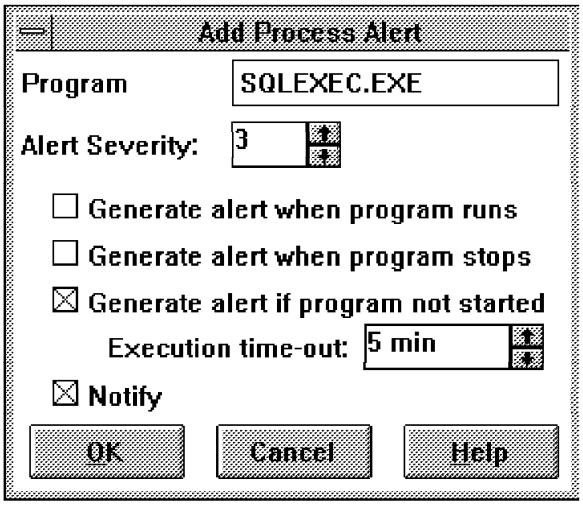


Figure 137. Process Manager - Add Process Alert

3.2.6.7 Remote System Manager

With the Remote System Monitor all active remote systems can be administrated. An alert can be generated if a system is online or offline. These alert conditions are set for every individual system. A default system notification profile can be set for newly added or discovered systems. Existing systems will not be affected by changes in these profiles. A default profile can be set globally or for every group individually.

To define an alert condition for an individual system do the following:

1. Start the **Remote System Manager**.
2. Open the group containing the desired system.
3. Click with the right mouse button on the icon of the system.
4. Choose **System Notifications**.
5. Check the boxes to generate the alert if system is online and/or system is offline.
6. Set the **Presence Check Interval** to the time between two presence checks.
7. Click **OK** to set the alert condition.

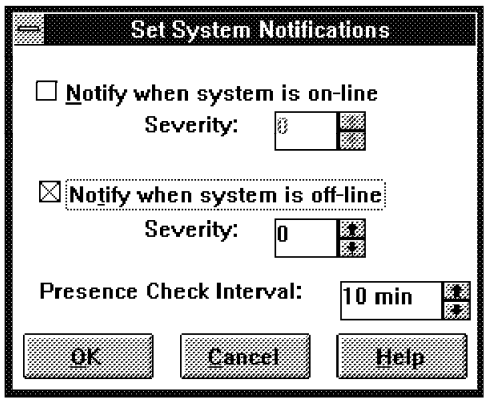


Figure 138. Remote System Monitor - Set System Notification

To define a global default alert condition profile do the following:

1. Start the Remote System Manager.
2. Choose **Options** and **System Notification Defaults**.
3. Check the boxes to generate the alert if system is online and/or system is offline.
4. Set the Presence Check Interval to the time between two presence checks.
5. Click on **OK** to set the default alert condition profile.

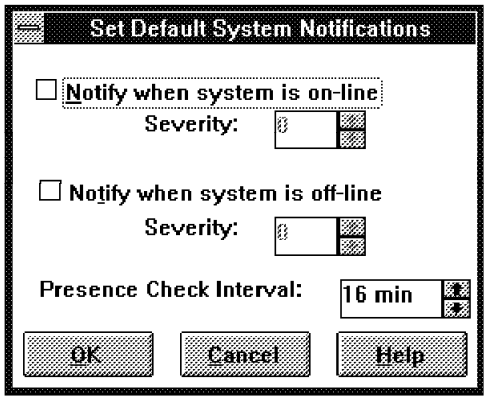


Figure 139. Remote System Monitor - Set Default System Notification

To define an alert condition profile for a system group do the following:

1. Start the **Remote System Manager**.
2. Click with the right mouse button on the icon of the group.
3. Choose **Group Notifications Defaults**.
4. Check the boxes to generate the alert if system is online and/or system is offline.
5. Set the **Presence Check Interval** to the time between two presence checks.
6. Click on **OK** to set the group default alert condition profile.

If you leave the default values, the values from the global profile will be used. This means, if the global profile is changed, the group profile will also change.

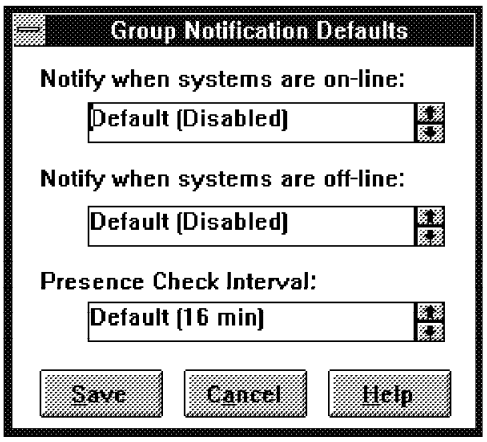


Figure 140. Remote System Monitor - Set Group System Notification Defaults

Warning

Consider that a short Presence Check Interval will generate a lot of network traffic, especially if you check on multiple systems.

3.2.6.8 Service Manager

The Service Manager controls the TME 10 NetFinity services. It can generate an alert for each time a service or the Service Manager itself is started. This must be enabled in the Network Driver Configuration for the entire system.

To set the configuration for Service Manager Alarms do the following:

1. Start the **Network Driver Configuration** from the TME 10 NetFinity group.
2. Click on the **Options...** button to open the Options window.
3. Check the **Service Execution Alerts** box.
4. Click on **OK** to save the setting.
5. Click on **Exit** to leave the Network Driver Configuration.
6. Restart the TME 10 NetFinity Support Program.

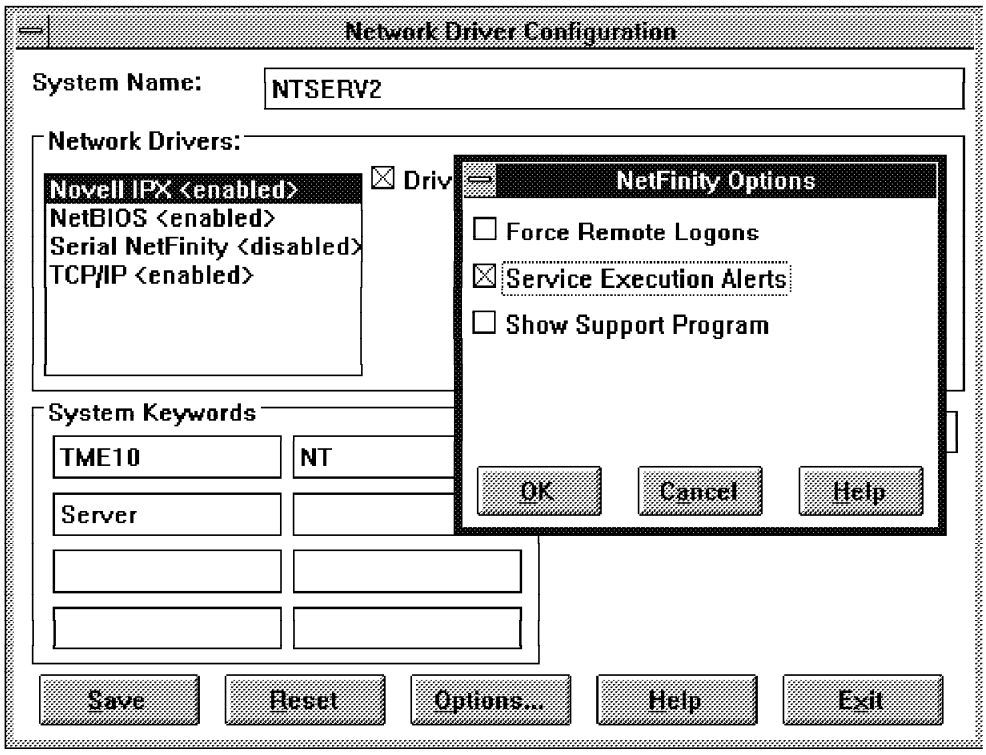


Figure 141. Network Driver Configuration - Options

3.3 Alerts by Windows NT Performance Monitor

Windows NT Performance Monitor is a part of the Windows NT system. It can supervise a wealth of system functions of Windows NT on the local or remote system. See 2.2.2, “Windows NT Performance Monitor” on page 56 for more details about NT Performance Monitor. This chapter only covers the alerts generation and forwarding.

Alerts in Windows NT are triggered from the controller in defined time intervals. There is no agent needed to assist or perform the monitoring. Therefore, no triggering from a controlled system or process is possible.

3.3.1 Alert Generating

You can create an alert profile by defining one or more alerts from various groups for the local and/or multiple remote systems and save this profile to a .PMA file on the managing system.

To define a profile do the following:

1. Open **Windows NT Performance Monitor**.
2. Choose **View** then **Alert**.
3. Choose **Edit** and **Add to Alert** or click on the + button.
4. Select the computer name from the system you would like to supervise.
5. Select an object group.
6. Select desired counter and, if applicable, the instance.
7. Assign a color to identify the alert.

8. Define a threshold condition in the Alert if field.
9. Insert a program name or command in the Run Program on Alert field if desired.

   Repeat this procedure for all alerts in the profile.
10. Choose **Options** and **Alert** from the top menu.
11. Set the interval time (time between two checks on the alert trigger).
12. Insert a network name if you would like to forward the alert through Messenger Service.
13. Check Log Event in Application Log if you would like to have an entry for each alert in the Windows NT Application Log file.
14. Choose **File** and **Save Alert Settings as** from the top menu and assign a file name to save the profile.

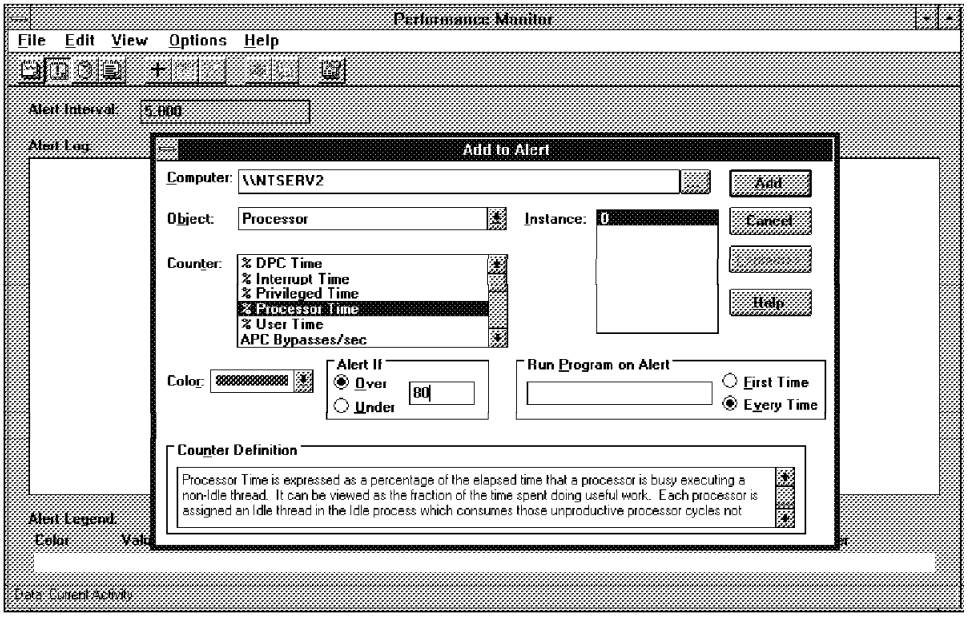


Figure 142. Windows NT Performance Monitor - Add to Alert

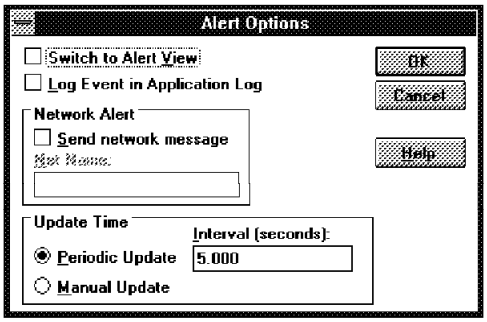


Figure 143. Windows NT Performance Monitor - Alert Options

Multiple Profiles on Same Manager System

If you would like to have multiple profiles on the same system simultaneously active, you can start the Performance Monitor multiple times as separate

instances. This might be desirable, because there is only one interval time setting per profile possible.

3.3.2 Alert Forwarding

Windows NT Performance Monitor has very limited ability to forward alerts. It can do so in the following ways:

- A run command statement can be defined to be executed either every time an alert is triggered or only the first time. This can be set up for each alert separately.
- The alerts can be logged to the Windows NT application log file to be viewed with the Event Viewer. This can be defined only for the whole profile.
- A message can be sent through the Windows Messenger Service to another system which can communicate with this service. This also can be defined only for the whole profile.

Besides the ability of the Performance Monitor to forward alerts, system alerts can be forwarded by the system itself. To configure this, do the following:

1. Open the **Server Manager** from the Administrative Tools Group.
2. Select the system you like to forward the alarms from. If it is in another domain, select the domain by choosing **Computer** then **Select Domain** and open the domain the system is belongs to.
3. Choose **Computer** then **Properties** and click on the **Alerts** button.
4. Enter the computer name or user name of the receiver in the left field and click on **Add**. You can add multiple names this way.
5. Click on **OK** and close all windows.

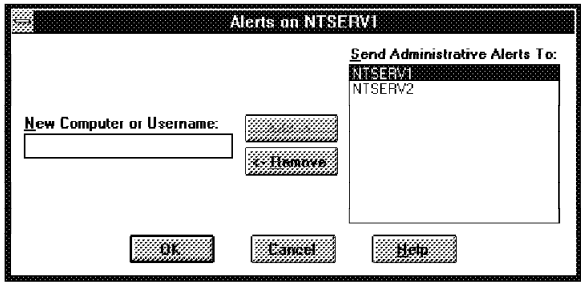


Figure 144. Windows NT System Alerts Forwarding

Warning

If a remote system is down, the Performance Monitor will create an alert `Computer not responding...`. However, the system will be checked every time interval and if it is still not responding, the checked value is assumed to be 0. This may lead to misleading alert messages.

Chapter 4. Managing Clients

Examples of managing clients from the NT platform are shown in this chapter. We tested the functionality of the TME 10 NetFinity Manager running under Windows NT accessing the clients running under different operating systems. The clients were on the following platforms:

- Windows NT 3.51
- Windows 95
- Windows 3.11
- OS/2 Warp
- OS/2 LAN Server
- NetWare 4.1

4.1 Installation and Configuration

The installation and configuration of the different clients is very similar. The configuration, which has already been described in 1.3, “Installation under NT” on page 3, shows all the steps for a complete installation of NetFinity clients. Depending on the operating system and the supported LAN device drivers, there might be a difference for the supported network protocols.

TME 10 NetFinity under Windows NT as well as under OS/2 supports the same network protocols (TCP/IP, NetBIOS, IPX, and serial connections). There is no limitation. You may use any of the protocols and connections that were already described in 1.2, “Hardware and Software Requirements under NT” on page 1.

4.1.1 Windows 3.1 and Windows 95 Installation

TME 10 NetFinity under Windows 95 supports all network protocols. There is no limitation. This of course depends on the LAN device drivers, which have been installed under Windows. For example if you have the NetWare for Windows client installed and you have also defined NetBIOS from NetWare as a network protocol, then this NetBIOS cannot be used for TME 10 NetFinity. Only IBM NetBIOS and IBM-compatible NetBIOS is used. With IBM NetBIOS, TCP/IP, IPX, serial device support and the Webabilty feature, there were no problems.

4.1.2 NetWare Installation

TME 10 NetFinity under NetWare supports TCP/IP and IPX as a network protocol to access a NetWare server as a NetFinity client. The NetWare NetBIOS protocol is not compatible with IBM NetBIOS protocol and therefore it cannot be used to access a NetWare server. The Internet connection protocol might also be used to access the server, but not directly, because to configure and access a workstation using the Internet interface requires the TME 10 NetFinity Manager product to be installed. For NetWare servers there is only the NetFinity Services product available. The only way to access a NetWare server over the Internet is going through another managing workstation, which is then connected to the Internet.

The installation is done by running the NETFINST NLM on the NetWare 3.x or 4.x server from the first NetFinity for NetWare diskette. The installation process

© Copyright IBM Corp. 1996

under NetWare does not use a graphical user interface, because native NetWare 4.1 does not support it. The installation process is simply in a text mode only. It still gives you the full functionality of installing and configuring the NetFinity services. At the end of the installation process you will also be asked for the configuration information such as network protocols, names and keywords. You can define them on this text mode screen or you change your configuration later from your managers workstation using the remote system manager service.

4.2 Functions and Differences

Most of the TME 10 NetFinity Services are identical on all client platforms. There are only a few exceptions from this. The major difference from a functionality point of view is within the Monitor service of NetFinity. These differences can be seen in a table later on in this chapter. See 4.3, “Summary” on page 119 for details. For more information on the other functions, have a look at the following sections, where we show the functional differences, if there are any, for each client operating system. These differences are compared to the functions supported by a Windows NT client.

4.2.1 Windows 95 and Windows 3.11

Services under Windows 95 and Windows 3.11 have full functionality without any limitations. Only within the monitor services are there some differences, which you can see in 4.3, “Summary” on page 119. All other services are identical to those running under NT.

4.2.2 OS/2 Warp

OS/2 Warp does not have any limitations within the functionality compared to Windows NT. It also does not matter if there is LAN server/requester software installed or not. The only difference between running LAN server software and not running it, from the NetFinity point of view is in the monitoring service. In the summary at the end of this chapter you can see the details about the monitoring differences.

4.2.3 NetWare

Under NetWare there is only the NetFinity Services product and not the manager available. So the NetWare server is only used as a client for NetFinity and not as a managing workstation. You cannot use the NetFinity services locally on the NetWare servers, because you don’t have any graphical user interface supported on NetWare servers. You need the GUI to control the NetFinity services. From a managing workstation you can access the NetWare server using NetFinity services without any limitations. The amount of information you receive depends on the other operating system of the hardware architecture.

A difference between the NT client and the NetWare client is related to the NetWare architecture. Normally you have a small DOS partition which is used to boot from and to load the server software. Once the NetWare server software is loaded, you should not have access to the DOS partitions. With the critical file monitoring service you are able to monitor the possible access to the DOS partitions and its files.

In addition, there is no File Transfer Service available from and to a NetWare server.

The Remote Session Service does not start a DOS session in the background of the NetWare servers, but it gives you control of the system console of the NetWare server. This is very similar to the RCONSOLE function of NetWare, but you are not able to switch to a different task in your NetWare server. For example, if your server console is currently showing the NetWare monitor, then you can work within the monitor, but you are able to switch to the server system console. The problem is the identical keyboard functions under NT and NetWare. CTRL-ESC is used under NT to switch to the NT task list, and under NetWare you are using the same key combination to access the current screen list. You then have to end the monitor service and you will be back on the main NetWare console.

We experienced another limitation in this environment. Under the NetWare server you are not able to use the Internet connection to directly access the NetWare server. This is because you need a NetFinity Manager package to run the Web interface and there is only a NetFinity Services product available for NetWare servers. Of course you can indirectly connect to the NetWare server via another NetFinity Manager in the same LAN.

4.3 Summary

The major differences between the clients under NetFinity are the functions within the monitor services. The following summary shows the differences of the monitor functionality when accessing different clients under different operating systems. The X in a column means, that this information can be retrieved from this client via the monitor service. There are some differences depending on the operating system.

Table 1 (Page 1 of 2). Monitor Functions by Operating Systems

Function	Windows NT 3.51	Windows 95	Windows 3.1	OS/2 Warp	OS/2 LAN Server	NetWare 4.1
CPU utilization	x	x	x	x	x	x
Process count		x	x	x	x	x
Thread count				x	x	x
Integer instruction rate					x	
Floating point operation rate					x	
Interrupt rate					x	
Port I/O rate					x	
Memory I/O rate					x	
CPU cache hit rate					x	
Disk/volume space used	x	x	x	x	x	x
Disk/volume space remain	x			x	x	x
Disk/volume workload	x		x	x	x	
Disk drive error rate	x	x	x	x	x	x
Print jobs queued				x	x	
Locked memory	x	x	x	x	x	
Memory usage	x	x	x	x	x	
Swap file size				x	x	
Swap space remaining				x	x	
Windows resource usage		x	x			
Percentage of cache in use						x
Cache blocks in use						x
TCP/IP						
Unicast packets sent	x			x	x	x
Broadcast packets sent	x			x	x	x
Bytes sent	x			x	x	x
Unicast packets received	x			x	x	x
Broadcast packets received	x			x	x	x

Table 1 (Page 2 of 2). Monitor Functions by Operating Systems

Function	Windows NT 3.51	Windows 95	Windows 3.1	OS/2 Warp	OS/2 LAN Server	NetWare 4.1
Bytes received	x			x	x	x
UDP datagrams sent	x			x	x	x
UDP datagrams received	x			x	x	x
IP packets sent	x			x	x	x
IP packets received	x			x	x	x
IP packets received with errors	x			x	x	x
TCP connections	x			x	x	x
TCP/IP sockets				x	x	x
LAN Server						
Sessions	x				x	
Connections					x	
Opens	x				x	
Shares	x				x	
Bytes sent	x				x	
Bytes received	x				x	
Response time					x	
Req.Buffer shortage					x	
Big Buf.shortage					x	

Chapter 5. TME 10 NetFinity Database Support

This chapter shows the different databases supported for TME 10 NetFinity and how they can be implemented.

You can access databases from Windows applications in the following ways:

- Through a database client either on the workstation or as part of the application.
- Through the Microsoft Open Database Connectivity (ODBC) interface driver.

However, TME 10 NetFinity will use the access through the ODBC interface even if it used the direct access in older versions of NetFinity. See 5.4, “TME 10 NetFinity with Direct Access to the IBM DB2 NT Database” on page 140 for more information about direct database access.

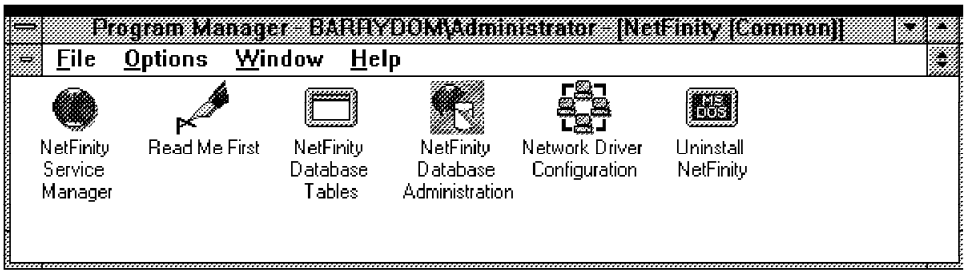


Figure 145. TME 10 NetFinity Main Window

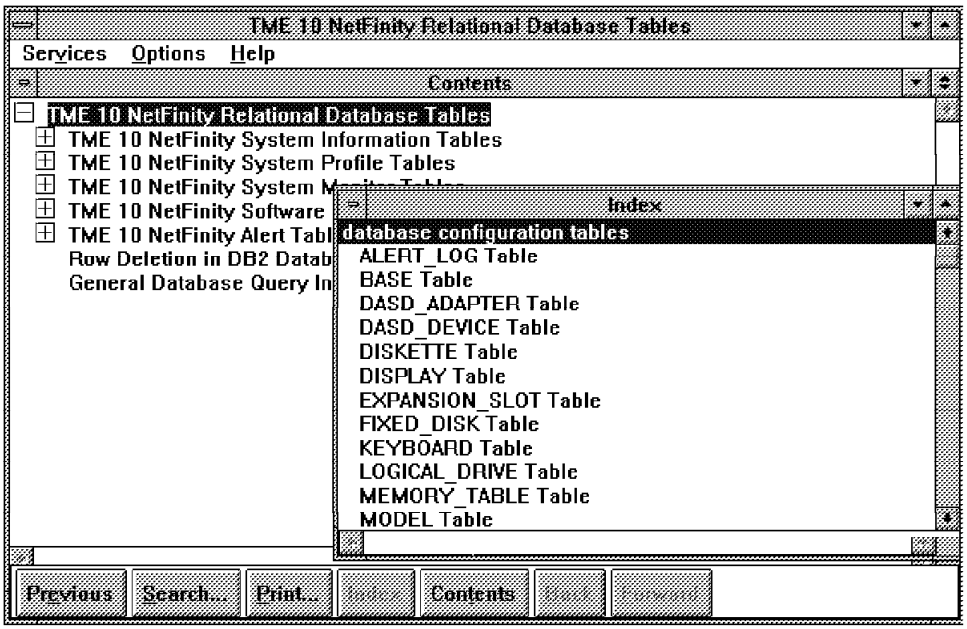


Figure 146. TME 10 NetFinity DB2 for NT Help

© Copyright IBM Corp. 1996

5.1 Database Support with ODBC Drivers

This section shows the new ability of TME 10 NetFinity to use the ODBC interface. ODBC drivers in Windows allows you to access many different database products through a standardized interface.

Microsoft′s ODBC provides a common SQL (Structured Query Language) syntax for communication between applications and database management systems (DBMS). Depending on the DBMS, the driver interprets the SQL statement from the application and translates it to the appropriate statement for the DBMS. Through the appropriate driver, even non-SQL DBMS such as DBASE or even flat files can be handled as if it were SQL data source, within applications.

With the implementation of the ODBC interface into TME 10 NetFinity, a much wider range of databases is supported. Theoretically, every database that provides an ODBC driver for Windows NT is accessible from TME 10 NetFinity.

There is still the possibility to export the data to the IBM DB2 database directly in the same way as in NetFinity for OS/2.

5.2 TME 10 NetFinity with IBM DB2 for Windows NT Using ODBC

This section leads you through the steps required to enable data to be exported from TME 10 NetFinity into an IBM DB2 for Windows NT database through the ODBC Interface Driver.

5.2.1 Setup DB2 for Windows NT and Create Database

Before you start the installation, make sure you are logged on to Windows NT with administrators rights and with a user ID that is less then 8 characters. Therefore, using the Administrator user ID would not be a valid choice. You may need to create a new ID with administrator rights.

1. Install IBM DB2 for Windows NT on the TME 10 NetFinity Manager System.

   You can either install from diskettes, CD ROM or a LAN drive. For detailed information about installing DB2 refer to *IBM Database 2 for Windows NT, Installation and Operation Guide, Version 2*, S33H-0312-00.

2. Create the database instance.

   For starting the database automatically on a server, it must be defined as a unique instance to the system. Use the DB2ICRT.EXE tool in the \SQLLIB\BIN directory to create this instance with the instance name. This name must not interfere with Windows NT service names and must follow the directory name convention (without extension). Use the format DB2nnnnn, where nnnnn is your chosen name. The following command will create a DB2 instance with the name DB2NETFS:

   ```
   DB2ICRT DB2NETFS
   ```

3. Configure DB services to start automatically.

   For productive environments the DB Services must start automatically. To achieve this, set the Startup Type in the NT Service Manager for the Services DB2 - Instance name and DB2 Security Server to Automatic.

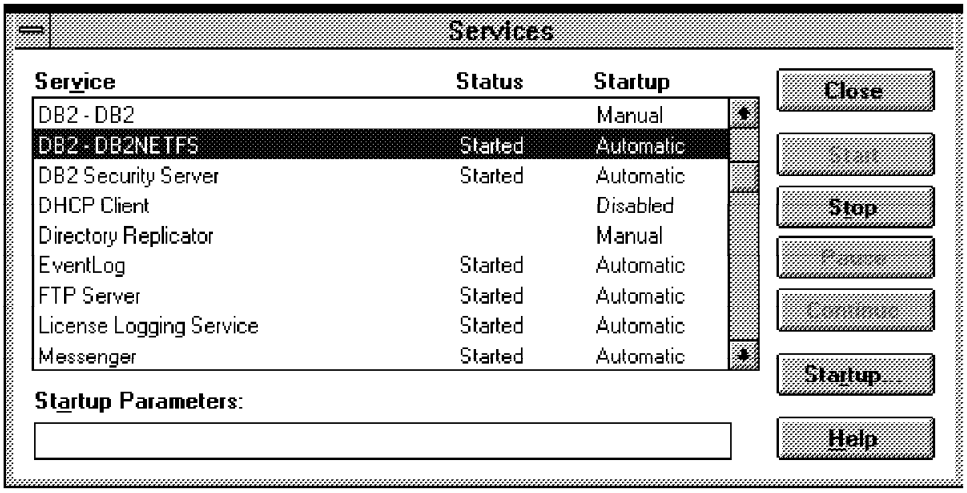


Figure 147. Automatic Startup of Database Services

4. Create a new database for the TME 10 NetFinity data.

   Open the DB2 Command Line Processor and enter the following commands to create a new database:

   - db2 => start database manager
   - db2 => create database NETFINS

   For more help about the DB2 Commands type ? command or refer to the online reference.

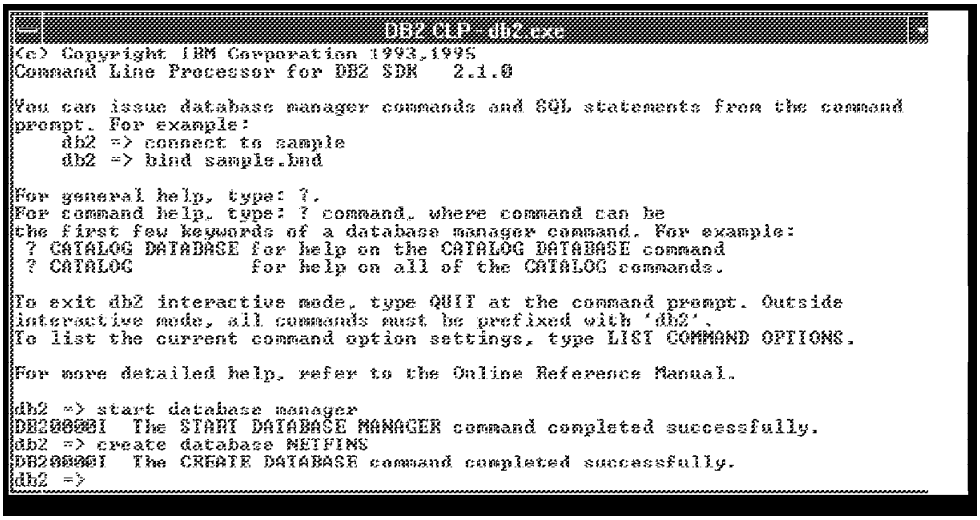

DB2 CLP - db2.exe
(c) Copyright IBM Corporation 1993,1995
Command Line Processor for DB2 SDK 2.1.0
You can issue database manager commands and SQL statements from the command prompt. For example:
db2 => connect to sample
db2 => bind sample.bnd
For general help, type: ?.
For command help, type: ? command, where command can be the first few keywords of a database manager command. For example:
? CATALOG DATABASE for help on the CATALOG DATABASE command
? CATALOG for help on all of the CATALOG commands.
To exit db2 interactive mode, type QUIT at the command prompt. Outside interactive mode, all commands must be prefixed with 'db2'.
To list the current command option settings, type LIST COMMAND OPTIONS.
For more detailed help, refer to the Online Reference Manual.
db2 => start database manager
DB20000I The START DATABASE MANAGER command completed successfully.
db2 => create database NETFINS
DB20000I The CREATE DATABASE command completed successfully.
db2 =>

Figure 148. Create DB2 Database NETFINS

5.2.2 Install and Configure DB2 ODBC Support

1. Start ODBC Installer form the DB2 for Windows NT window as shown below:

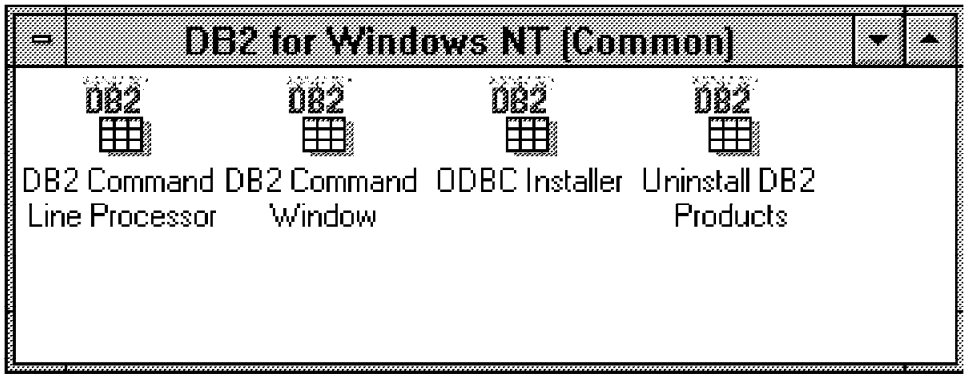


Figure 149. Create DB2 Database NETFINS

This installs the IBM DB2 ODBC Driver and creates a new Program Manager group with the name ODBC and puts the 32-bit ODBC administrator in it.

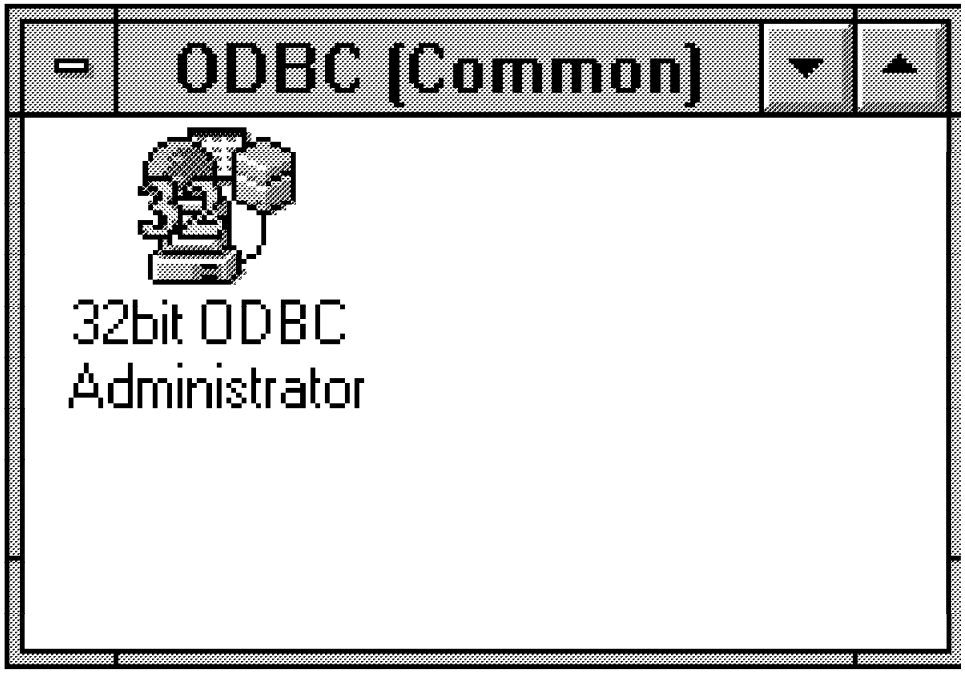


Figure 150. 32-Bit ODBC Administrator

2. Start the 32-bit ODBC Administrator from the newly created ODBC group.
3. In the Data Sources windows choose **Add...**.

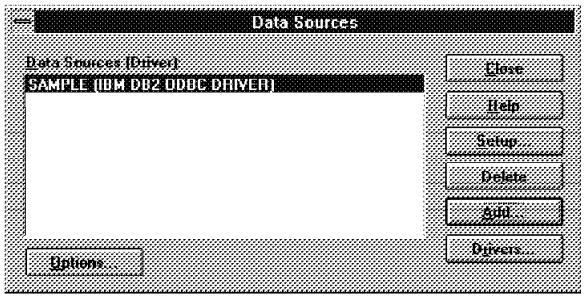


Figure 151. 32-Bit ODBC Administrator - Data Sources

4. From the installed ODBC drivers, choose **IBM DB2 ODBC DRIVER** and click on **OK**.

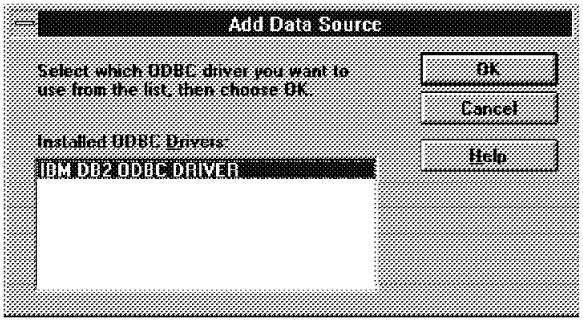


Figure 152. 32-Bit ODBC Administrator - Add Data Source

5. Select the newly created database in the Database Alias field and add a description in the Description field. Then click on **OK**.

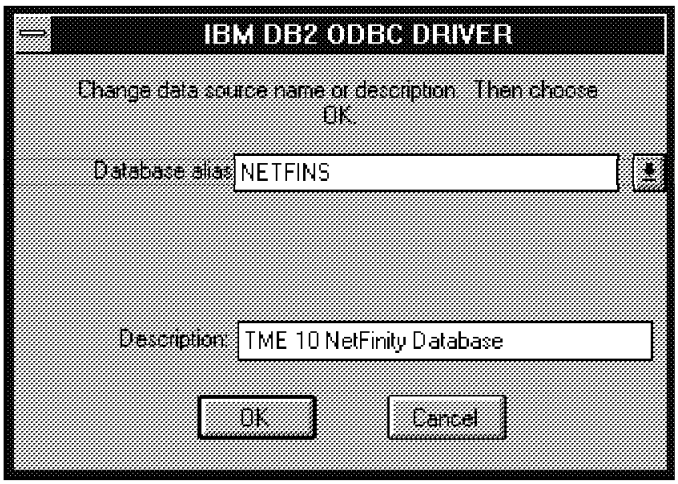


Figure 153. 32-Bit ODBC Administrator - IBM DB2 ODBC DRIVER

6. Close the Data Source window.

The IBM DB ODBC driver is now installed and the defined databases are available to all applications using the ODBC interface.

5.2.3 Create TME 10 NetFinity Tables through the ODBC Driver

TME 10 NetFinity Database Administration is used to add or delete tables needed for TME 10 NetFinity and to grant or revoke user's rights to the database.

1. Start TME 10 NetFinity Database Administration from the TME 10 NetFinity window and choose the following items:

   Select DBMS: IBM DB2 Using ODBC

   Specify Table Action: Create

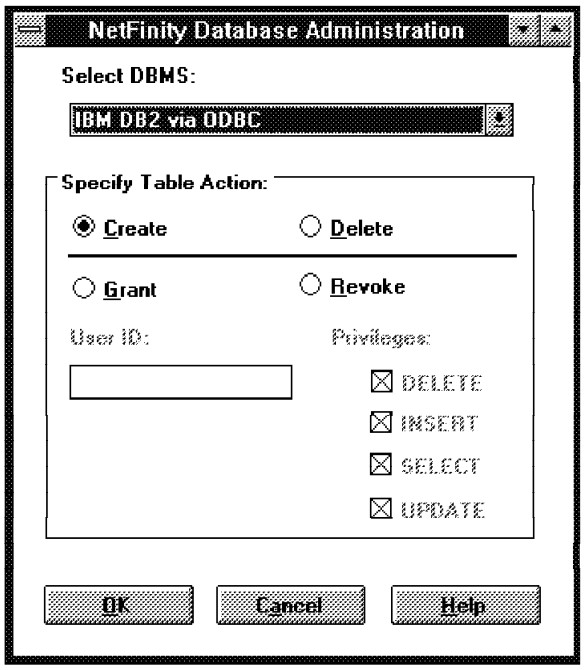


Figure 154. TME 10 NetFinity Administration

2. Choose the database to use with TME 10 NetFinity.

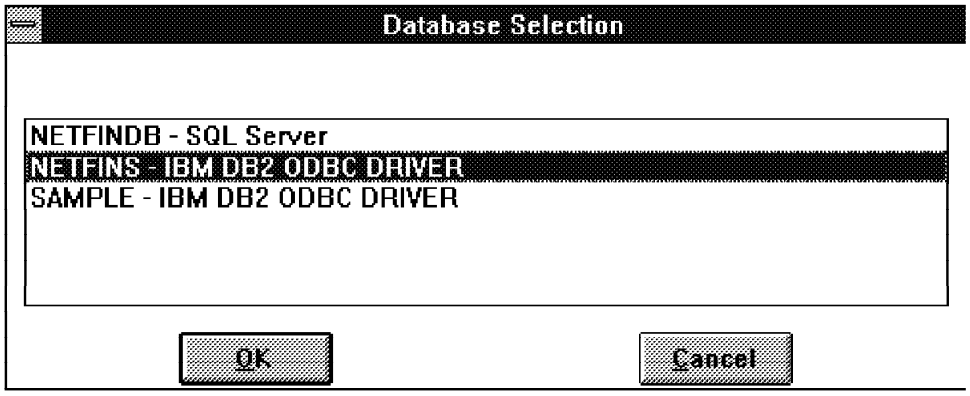


Figure 155. Database Selection

3. Enter the user ID and password to log on to the database.

   The user ID and the password depends on the database definition. This user ID must have the right to create and delete tables in the database. The user ID and password you were logged in with when creating the database is automatically granted the appropriate database access rights. If you would like to log on to the database with a different user ID, you must create this database user within the database configuration and grant the needed rights.

   Note

   You will have to go to the NT Administrative Tools and use the User Manager for Domains to add the NETFIN user ID.

   If you are using the Microsoft SQL database, use the same user ID and password as you used when you defined the TME 10 NetFinity database.

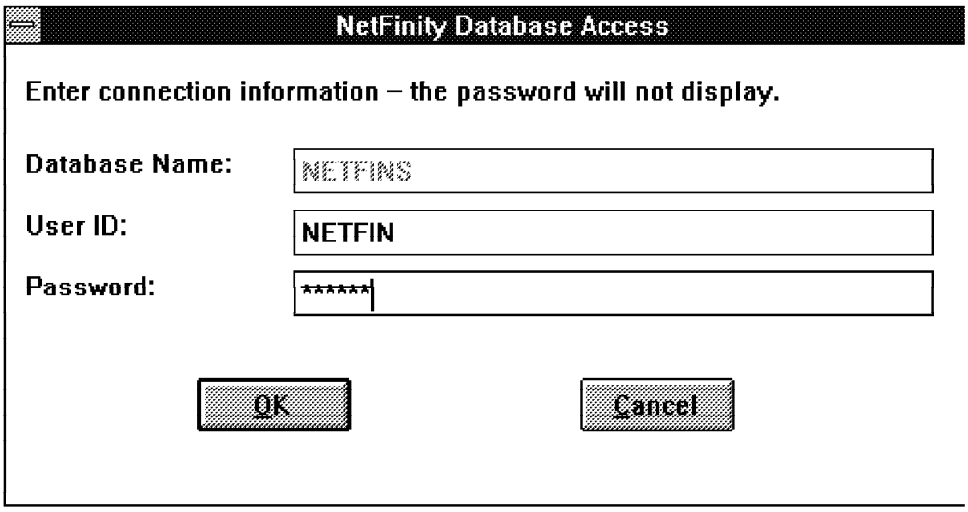


Figure 156. TME 10 NetFinity Database Access

4. Check the Results window for any errors. If no error occurred, the system will show you the following window:

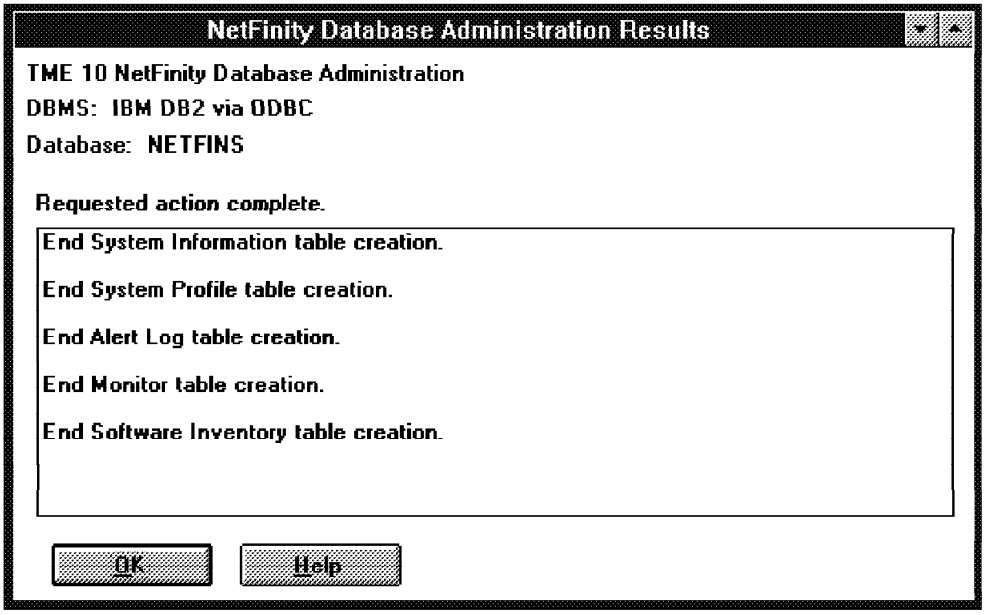


Figure 157. TME 10 NetFinity Database Administration Results

TME 10 NetFinity is now ready to export collected data to the DB2 Database for Windows NT. To check this, open **TME 10 NetFinity Service Manager**, start **System Information** and wait until the system has collected the data. From the System Information window choose **File** and **Database**.

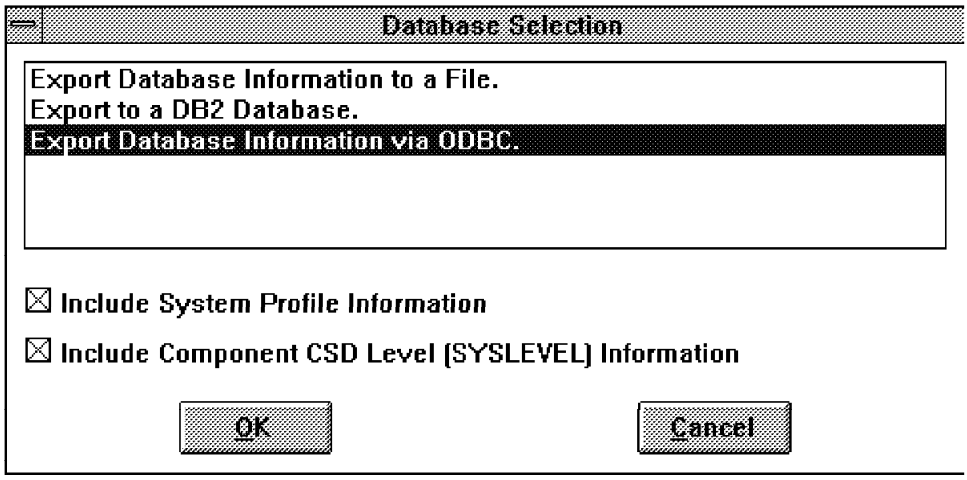


Figure 158. System Information Tool Data Exported

Note

The IBM DB2 ODBC Driver supports only 32-bit applications. With 16-bit applications the Microsoft 16-bit ODBC Driver must be installed. For how to work around the problems with a 16-bit Windows application check out the text file DB2ODBC.TXT in the \SQLLIB directory.

5.3 TME 10 NetFinity with Microsoft SQL Server Using ODBC

This paragraph leads you through the steps to enable the data export from TME 10 NetFinity in a Microsoft SQL server database through the ODBC Driver Interface. Some knowledge of Microsoft SQL server is assumed.

All screens and instructions refer to Microsoft SQL Server Version 6.0. We made a short test with Version 6.5 Beta. Some screens will differ but we encountered no problems with the setup described here.

The Microsoft SQL Server can either be installed on the managing system or on another MS Windows NT Server. To connect to an SQL database server on a different system, MS ODBC support and the Microsoft SQL ODBC Driver must be installed on the TME 10 NetFinity Manager and the Microsoft SQL Server must be defined for desired network communication.

5.3.1 Setup Microsoft SQL Server and Create Database

1. Install Microsoft SQL Server as described in the Microsoft Manual *SQL Server Setup*.

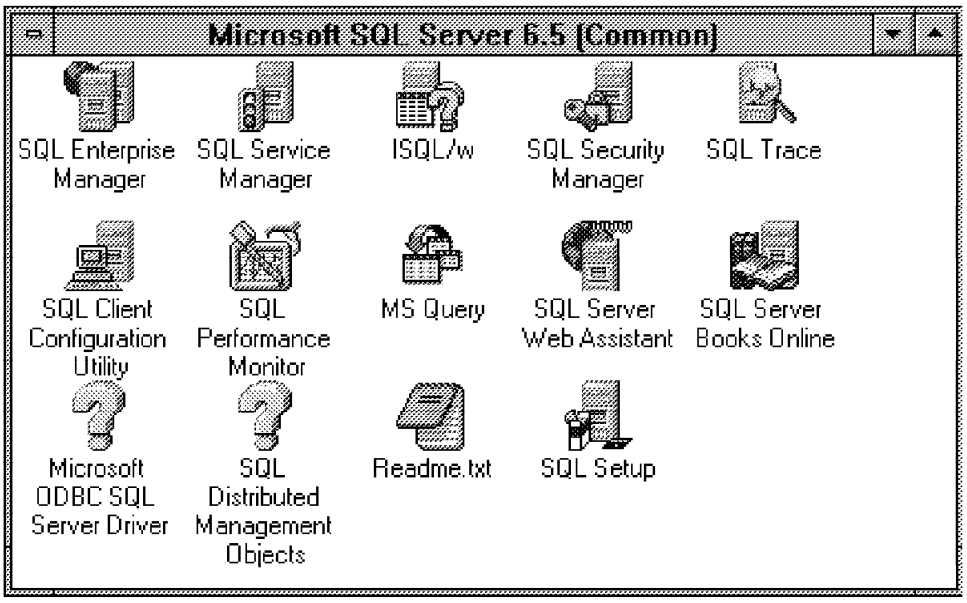


Figure 159. Microsoft SQL 6.5

2. On the SQL Server System start **Microsoft SQL Enterprise Manager**.
3. Register your server to the Enterprise Tree if it does not appear in the tree.
4. Click on your server in the tree and choose **Server** from the top menu.

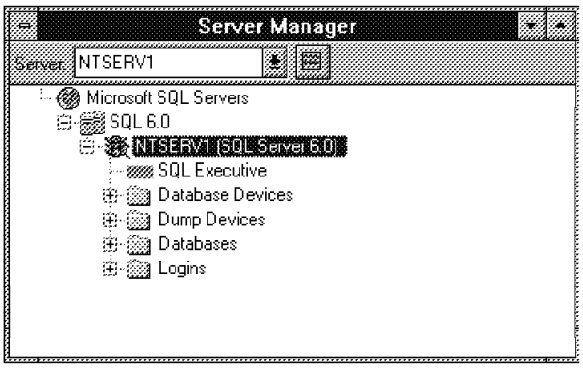


Figure 160. Microsoft SQL Enterprise Manager - Server Manager Tree View

5. Select **Configurations...** to open the Server Configuration window.
6. On the Server Options page mark the following:
   - Auto Start Server at Boot Time
   - Auto Start Executive at Boot Time

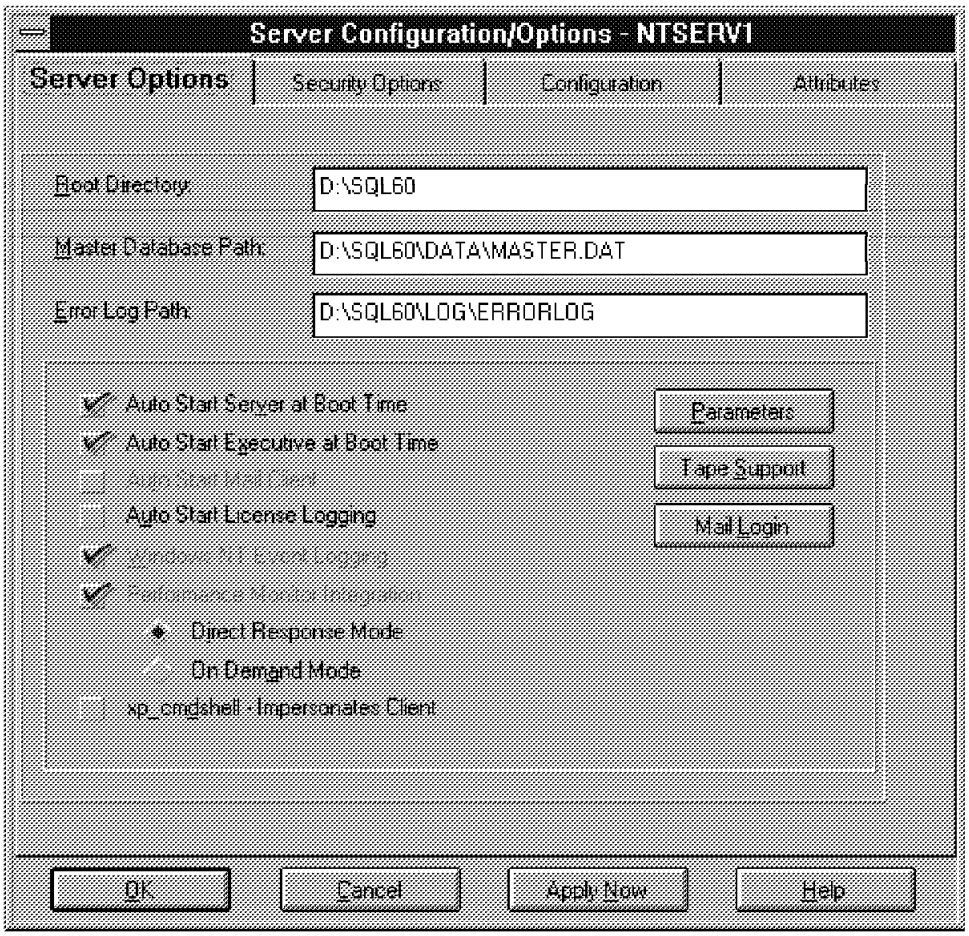


Figure 161. Microsoft SQL Enterprise Manager - Server Configuration, Server Options

7. On the Security Options page set Login Security Mode to Windows NT Integrated. This will allow all users defined in the domain or locally on the system to access the database.

Figure 162. Microsoft SQL Enterprise Manager - Server Configuration, Security Options

Next, you have to create a new database. For better performance it should be created on a separate device. A device is a part of the disk reserved for use by databases. Within this space multiple databases can be placed. For each database, you must allocate a place to store the data log itself and a place to store log entires. In our case the data and logs will be put into same device.

Before you create a device or a database, you should calculate the amount of space you will need. The size of the database depends on how many clients you intend to manage and how much data you are storing into the database.

As a rule of thumb, every client with hardware and software inventory data stored to a database will use approximately 50 KB of data space and 8 KB of log space.

If you intend to export data from the System Monitor, the amount of space per client can easily multiply. Do not define the device too small. Devices can be expanded or reseized if necessary but it is best to define the databases large enough to start with. Make sure you also leave room for expansion.

8. To create the database, highlight the server in the tree and choose **Manage** from the top menu. Then select **Databases...** and the Manage Databases window appears.

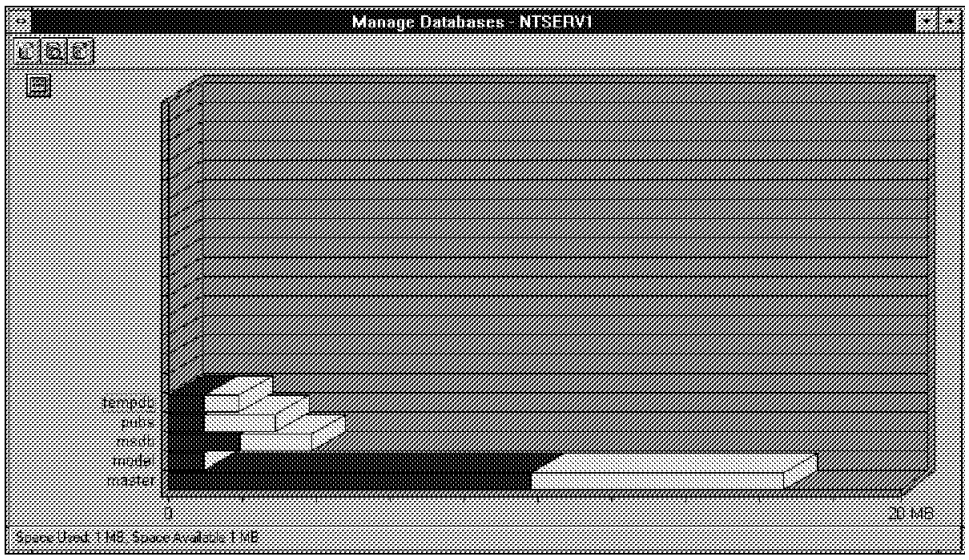


Figure 163. Microsoft SQL Enterprise Manager - Manage Databases

9. Click on the **New Database** icon (the left of the three icons in the upper left corner) to open the window to create a new database (see Figure 165 on page 135).

10. Choose **<new>** in the Data Device drop-down box and a window to create a new device will appear.

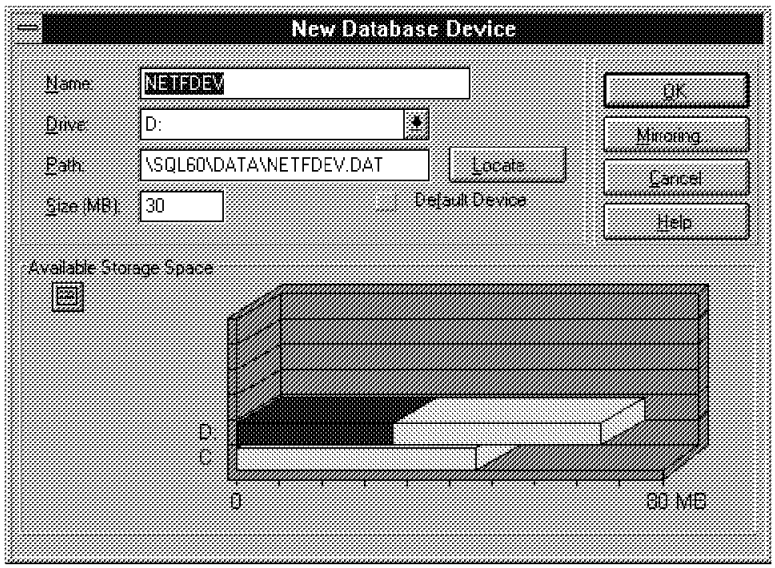


Figure 164. Microsoft SQL Enterprise Manager - New Databases Device

In the lower half of the window, the local drives with the available disk space for new devices is shown. Enter the name, drive, path and size of the new device in the appropriate fields in upper half and click on **OK** to create the device.

11. Back on the New Database window your newly created device is shown as an empty bar. Enter now the name and the size for the TME 10 NetFinity database. Choose the same device for the Log Device drop-down box and assign at least 15% of the database size to the log database. You can

already use the whole device or leave some space for further expansions of the database.

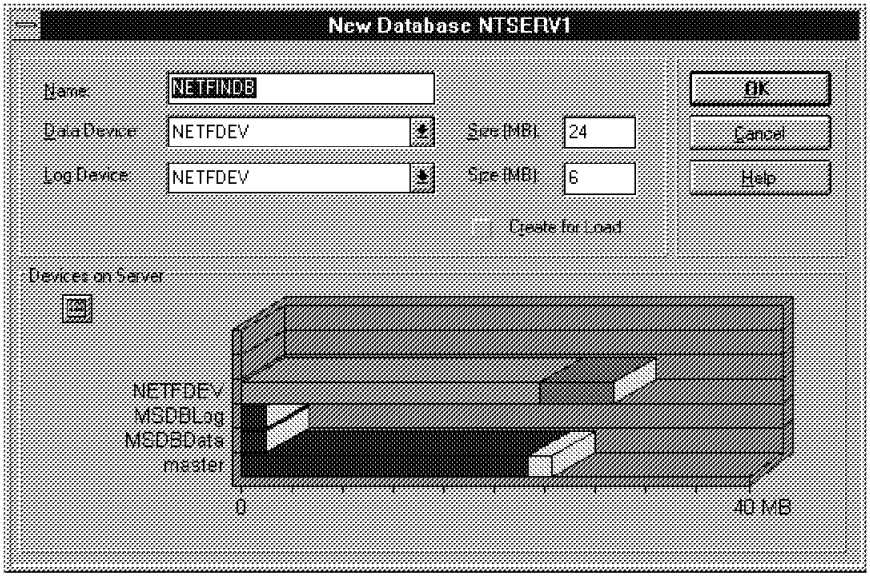


Figure 165. Microsoft SQL Enterprise Manager - New Database

If you click on **OK**, the database is created and should be shown in the Manage Databases window.

12. To enable TME 10 NetFinity to use the new database, a specific database user must be created with all access rights to the database. This user *must* be named NETFIN.

    Choose **Manage** and **Logins** from the top menu.

    Fill out the fields as shown in Figure 166 on page 136 and click on **Add** or, if the database user already existed, on **Modify**. Make sure you have **Permit** and **Default** checked for the TME 10 NetFinity Database and the Permit box for the Master database in the Database Access box.

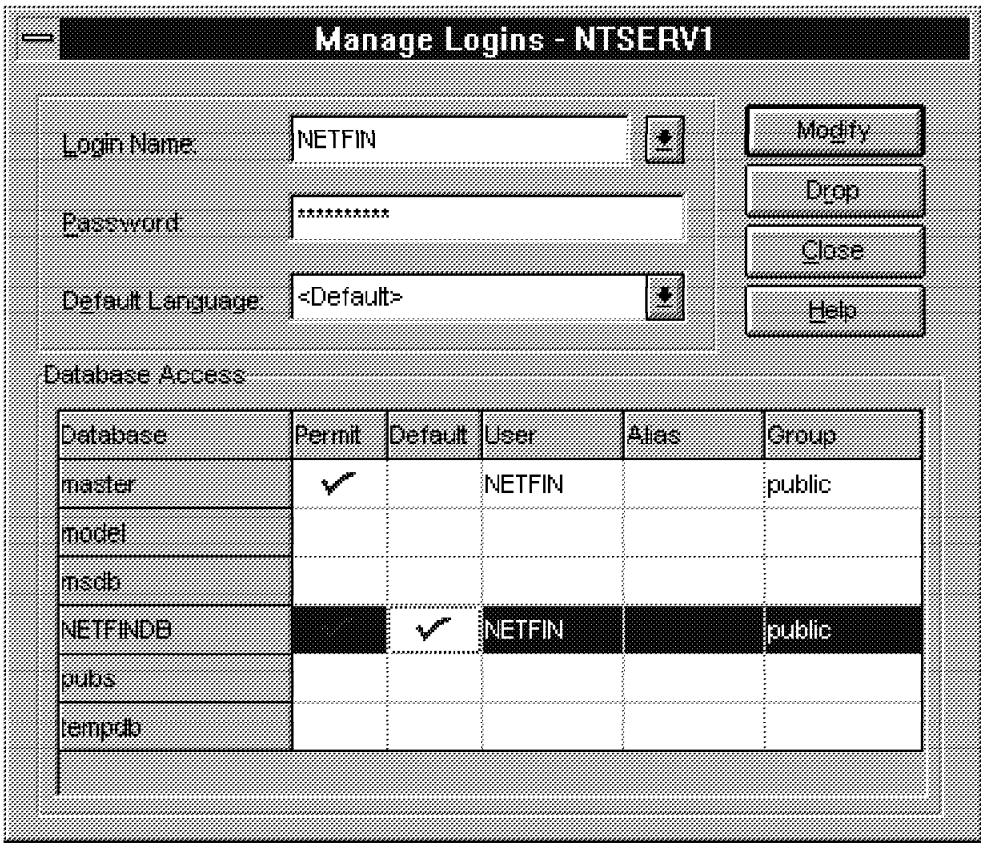


Figure 166. Microsoft SQL Enterprise Manager - Managing Logins

13. After creating the user, appropriate rights must be granted to it. Again select **Manage** and **Databases**. Double-click on the TME 10 NetFinity Database Name in the graphic to edit the database properties. Select the **Permissions** page and grant all rights to the NETFIN user as shown in Figure 167 on page 137. Click on **Modify**, then on **Close**.

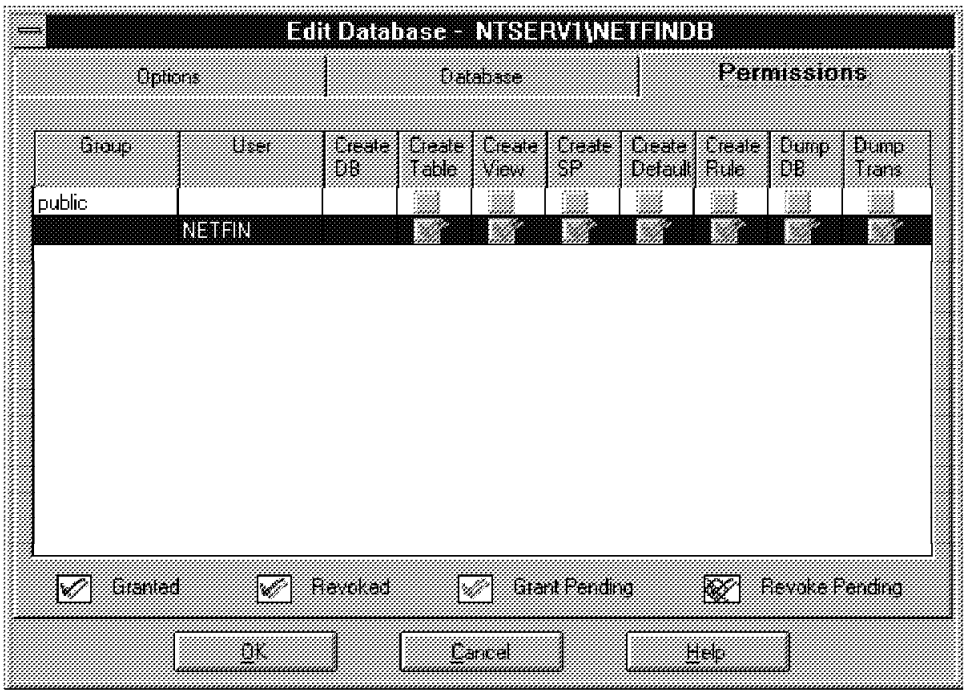


Figure 167. Microsoft SQL Enterprise Manager - Edit Databases, Permissions

14. Click on **OK** to close the Edit Database window and close the Microsoft SQL Enterprise Manager.

Looking at an SQL 6.5 view of the Server Manager, you would see the following:

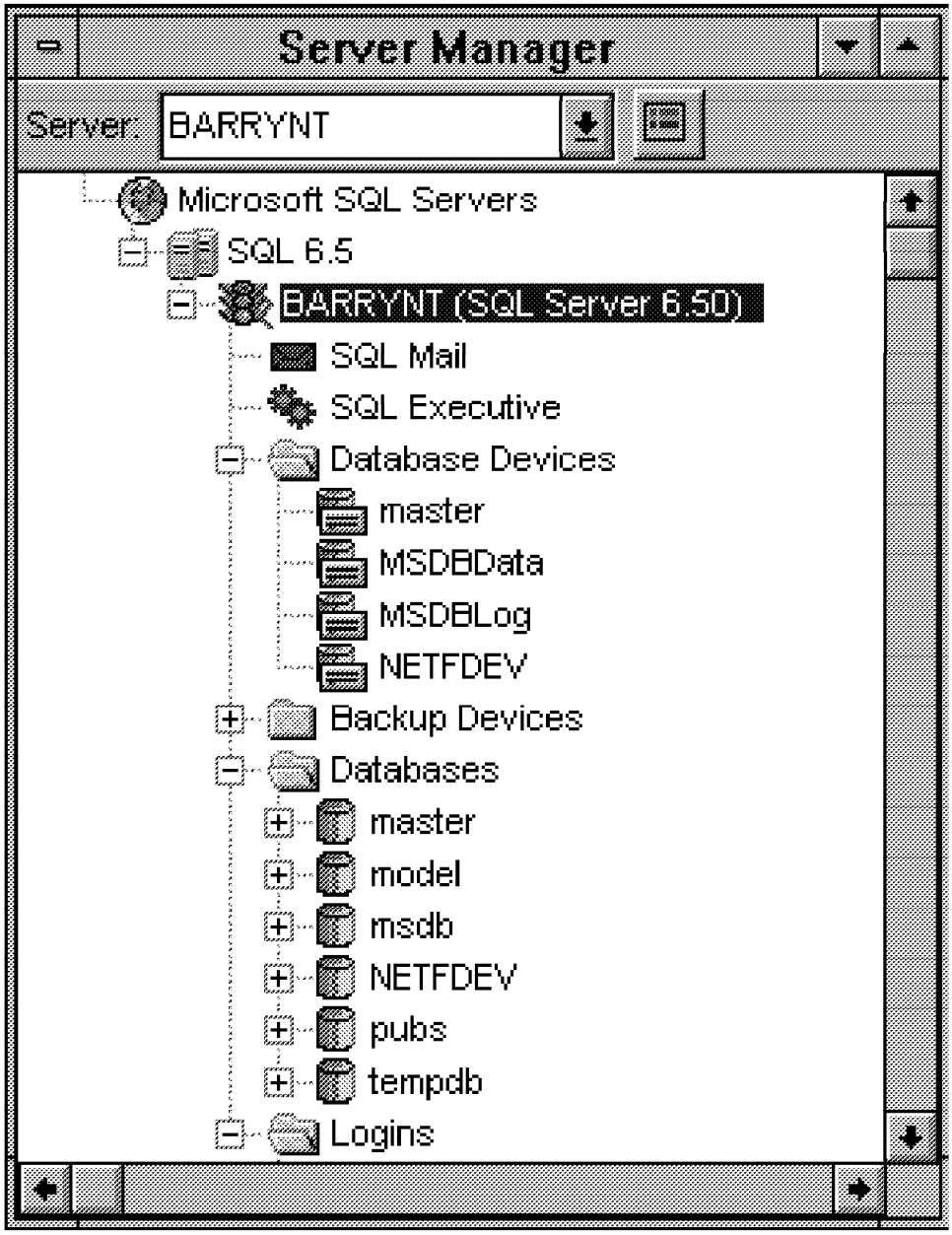


Figure 168. Microsoft SQL Enterprise Manager - Managing Logins

5.3.2 Install and Configure Microsoft ODBC Support

If the ODBC Support is not already installed, you need to install it from the SQL Server CD. After installation do the following to set up the database support:

1. Open the **Windows NT Control Panel** from the Main Group and choose **ODBC**.
2. In the Data Source window choose **Add**.
3. Choose **SQL Server** from the installed ODBC Drivers.
4. In the ODBC SQL Server Setup window (Figure 169 on page 139), click on **Options** to expand the Window and fill out the fields as follows:

Data Source Name:	Alias or name of the TME 10 NetFinity database
Description:	A brief description of the database
Server	LOCAL (Select the server name if you have Microsoft SQL Server running on another system and are connecting through the network.)
Database Name:	Name of the TME 10 NetFinity database in the SQL Server

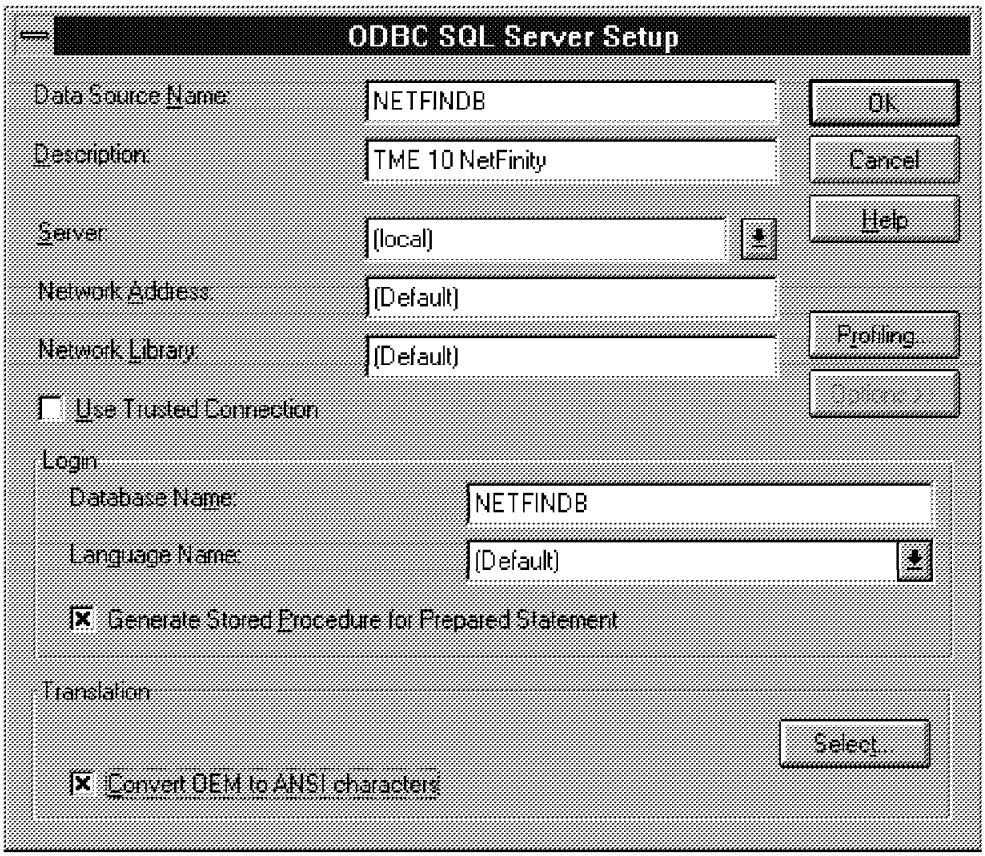


Figure 169. MS ODBC - ODBC SQL Server Setup

5. Close all windows and return to the Program Manager.

5.3.3 Create TME 10 NetFinity Tables through the ODBC Driver

To create the TME 10 NetFinity Tables in the Microsoft SQL Server database see 5.2.3, “Create TME 10 NetFinity Tables through the ODBC Driver” on page 127.

Use Microsoft SQL Server using ODBC instead of IBM DB2 using ODBC.

5.4 TME 10 NetFinity with Direct Access to the IBM DB2 NT Database

Since TME 10 NetFinity supports database access through the ODBC interface, direct access to the database is not supported anymore.

However, it still works the same as it has in older versions. The only problem is creating the database tables. The NetFinity database creation program NETFINDB.EXE is not included anymore in the delivered diskettes or CD install image. The only way for you to create the tables is through the ODBC interface. Thus, ODBC support has to be installed and configured. Since this is still a good way to save data, we covered it in this section.

TME 10 NetFinity will automatically recognize if a DB2 database server or client is installed on the system and shows the DB/2 databases to select in the Export to Database window.

However, you need to create the database, build the tables and views and bind the application package delivered with TME 10 NetFinity to the database to make all procedures available to the system. These procedures are stored in the package field DB2SQLC0.BND found in the \WNETFIN directory.

1. Create a new database for the TME 10 NetFinity data.

   Open the DB2 Command Line Processor and enter following commands to create a new database:

   ```
   db2 => START DATABASE MANAGER
   db2 => CREATE DATABASE NETFINS
   ```

2. Create the database tables through the ODBC interface with the TME 10 NetFinity Database Administrator as described in 5.2.3, “Create TME 10 NetFinity Tables through the ODBC Driver” on page 127.

3. Bind package to the database:

   - Start DB2 command line interface.
   - Connect to the TME 10 NetFinity database.

     ```
     db2 => CONNECT TO database-name
     ```

   - Bind package file and grant public access to the package.

     ```
     db2 => BIND drive\path\DB2SQLC0.BND GRANT PUBLIC
     ```

   - Reset database to activate package.

     ```
     db2 => CONNECT RESET
     ```

The database is now ready to store data from TME 10 NetFinity.

5.5 Export Data from TME 10 NetFinity to Database

There are several functions in TME 10 NetFinity that can export data to the database:

- System Information

  To save data to a database do the following:

  – Run the System Information service.

  – From the System Information top menu choose **File** and select **Database**.

– Select **Export Database Information via ODBC** and check the boxes if you would like to include the System Profile and/or Syslevel information.

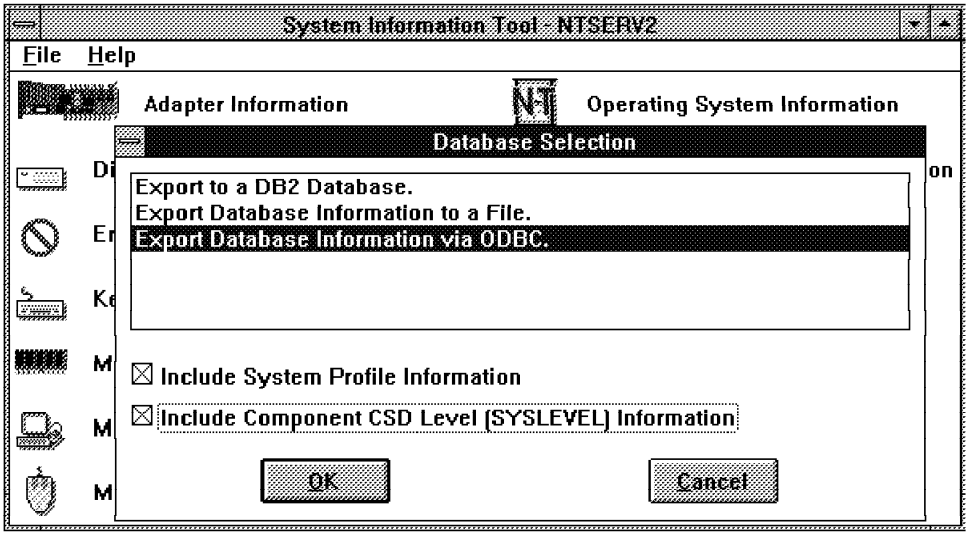


Figure 170. System Information - Database Export

– Select the database to export to and click on **OK** to save the data.

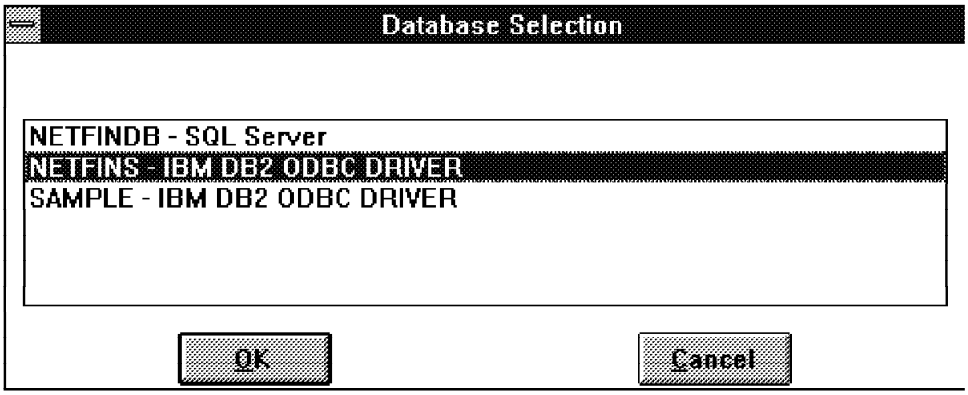


Figure 171. Database Selection

- System Profile

  The export of the System Profile data can be included while saving data from System Information.

- Software Inventory

  Software Inventory lets you save the search results to the database. To save this data do the following:

  – Run the Software Inventory service.

  – From the Software Inventory service top menu choose **Inventory** and select **Export to Database**.

  – Select **Export Database Information via ODBC**.

  – Select the database to export to and click on **OK** to save the data.

- System Monitor Service

System Monitor lets you collect data during a certain period of time and store them into the database. This data can later be used for reports.

To save data to a database do the following:

- Open the **System Monitor Service**.
- From the System Monitor Service top menu choose **Windows** and select **Export to Database**.
- Select the database to export to one or more monitors and define the time period to be monitored.

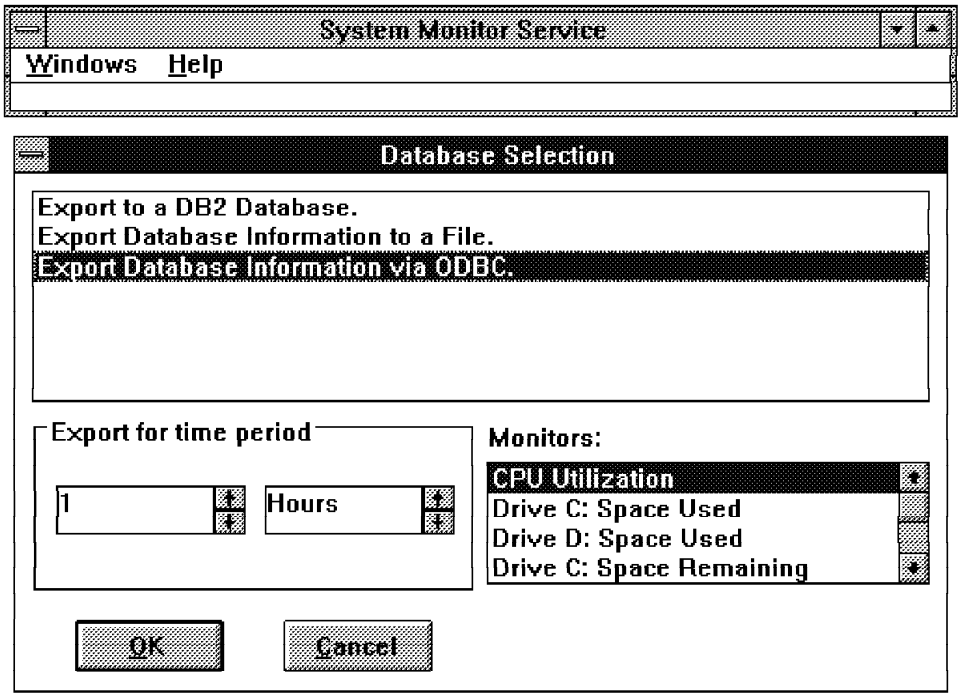


Figure 172. System Monitor Service - Database Export

- Select the database to export to and click on **OK** to save the data.

You can also save the data for a certain monitor by clicking on the right mouse button on the monitor itself and choose **Export to Database**.

- Event Scheduler Service

  If you run one of the services mentioned before from the Event Scheduler, you can also define to export the data to the database. Depending on the scheduled service, the database definitions had to be provided.

The first time you export to a database you will be prompted for a user ID and a password to log on to the database. TME 10 NetFinity stores this information and no further logon is required.

Data will always be exported to the local database even if you run a service through the Remote System Manager on a different system.

Remark

With WebFinity (Internet access to TME 10 NetFinity) export to database is not supported.

5.6 Query the TME 10 NetFinity Database

With TME 10 NetFinity no utility to query the database is provided. Depending on the database that contains the TME 10 NetFinity data, different programs can be used for example, to query Microsoft SQL Server Microsoft ISQL/w (provided with SQL Server) or Microsoft Query (provided with Microsoft Excel). The only tool provided with IBM DB2 for Windows NT is the DB2 Command Line Processor where you can enter SQL statements to query the database. But you can also use Microsoft Query or other programs that can access databases through the ODBC interface.

See the TME 10 NetFinity Relational Database Tables from the NetFinity Program Manager group for more information about the tables and definitions.

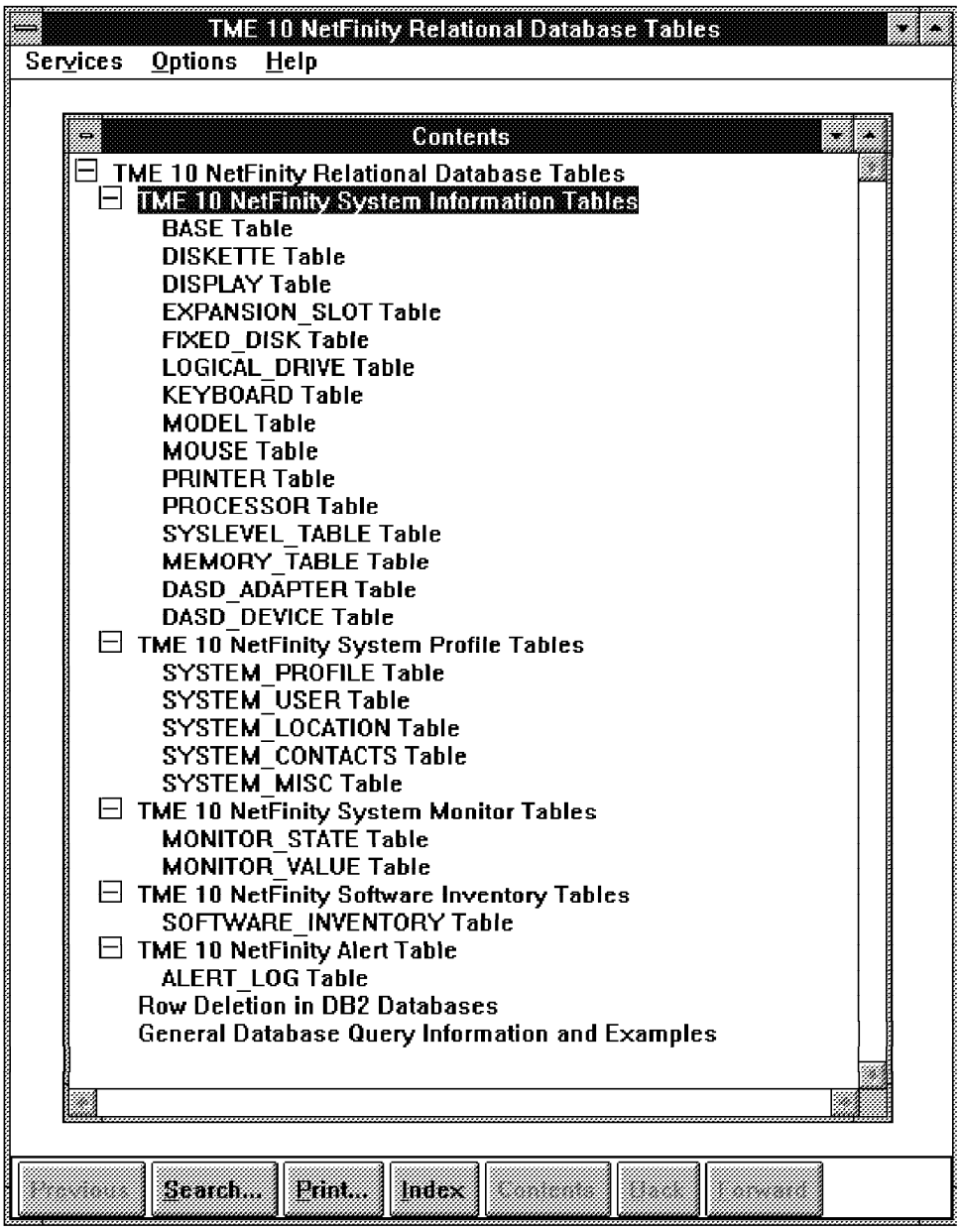


Figure 173. TME 10 NetFinity Relational Database Tables

Chapter 6. Webability

This chapter shows how to use a Web browser workstation to remotely manage your environment.

6.1 Internet Connections to TME 10 NetFinity

This chapter shows the different ways to connect from a managing workstation to remote workstations or LANs over the Internet using the TME 10 NetFinity 4.0 product. Having the possibility to manage workstations and servers using the World Wide Web gives you great flexibility for accessing system information independent of where the systems are physically located. You don't have to have a TME 10 NetFinity Manager installed at your local managing workstation. You can use the managing functions of the managing workstation at the remote site. In this case, you only have access to the TME 10 NetFinity managing services using the Internet from your local station, but not worry about other network protocols such as NetBIOS, TCP/IP or IPX. Figure 174 on page 146 shows the connections that may be used to get access to remote workstations. Within this chapter we call the system that provides the interface between the remote LAN and the Internet a *gateway*. This gateway also provides the data transfer and protocol conversion between the LAN and the Internet. It further provides the TME 10 NetFinity Manager services, because you don't have to have the NetFinity manager code installed at your local managing workstation, which has the Web browser installed. It also provides the security setup for accessing the remote LAN from a TME 10 NetFinity Manager using the Internet.

Please be aware, that if you are using the TME 10 NetFinity Manager using the Internet, TME 10 NetFinity works as a *nonsecure* Internet server. There may be a future version of TME 10 NetFinity which may provide the proper security features, but up to now with TME 10 NetFinity Version 4.0 from an Internet point of view, it is nonsecure. Of course all security features of TME 10 NetFinity are functioning and cannot be circumvented.

© Copyright IBM Corp. 1996

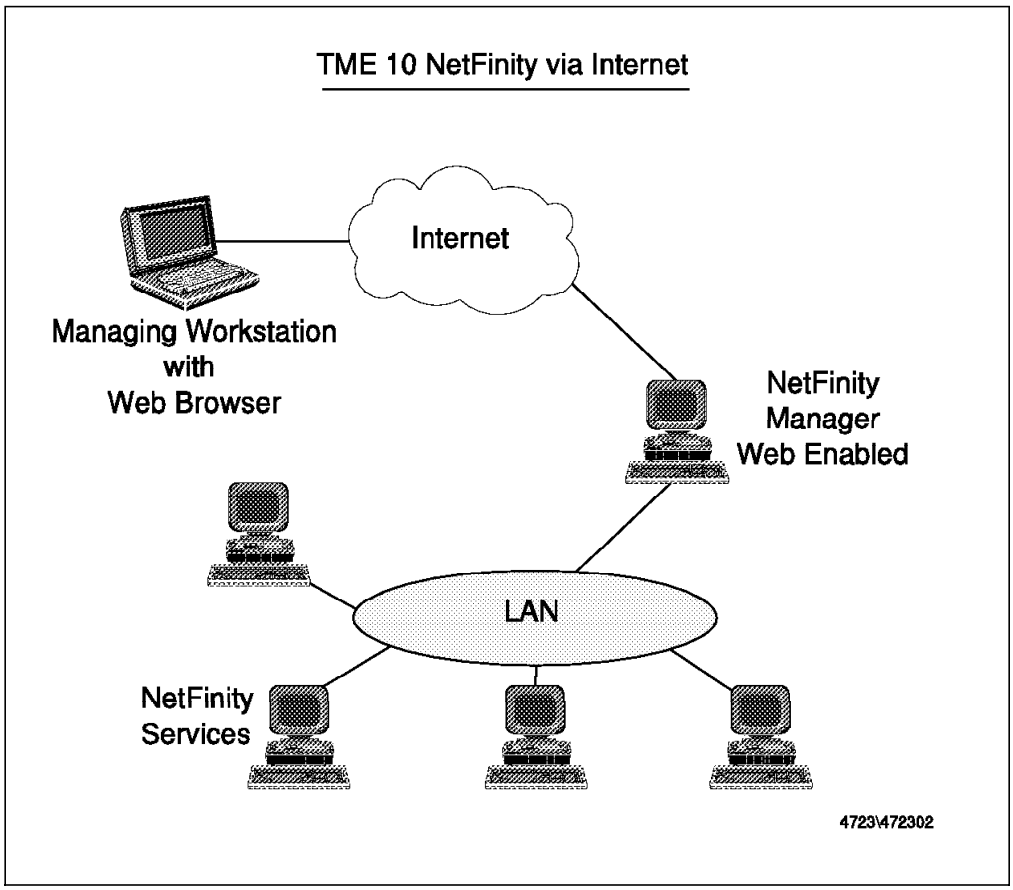


Figure 174. Internet Connection

There are some prerequisites for getting remote access. Of course you have to have a hardware connection to the Internet, which might be established in several ways, depending on your logical connection. Let's have a look at the different possibilities. For all of the possible connections to the remote site there are the following prerequisites for the local TME 10 NetFinity Manager:

1. NetFinity Manager code must *not* have been installed. If you are connected to the remote LAN using the Web browser, you are using the TME 10 NetFinity Manager from your remote managing workstation.
2. An Internet Web browser code has to be installed such as IBM OS/2 WebExplorer or Netscape. In our example we are using Netscape as a Web browser product. Since all information from the TME 10 NetFinity 4.0 manager is being sent as an Internet page including some GIF files, you can browse independent of the operating system. Therefore you may also use a Web browser running on a different system platform. For example, you may use an Internet Web browser running on a PowerPC-based system under AIX or NT.
3. Internet connection has been set up. This may be done by in the following ways:
   - Connecting to the Internet using your local Internet server.
   - Establishing the connection through a service providers network, such as logging on to CompuServe and then passing through to the Internet. In this case the Internet service provider gives you a valid Internet ID.

- Directly connecting to the Internet with a TCP/IP address provided by a service provider.

6.1.1 Accessing Remote LANs Using an Internet Server on the Remote Site

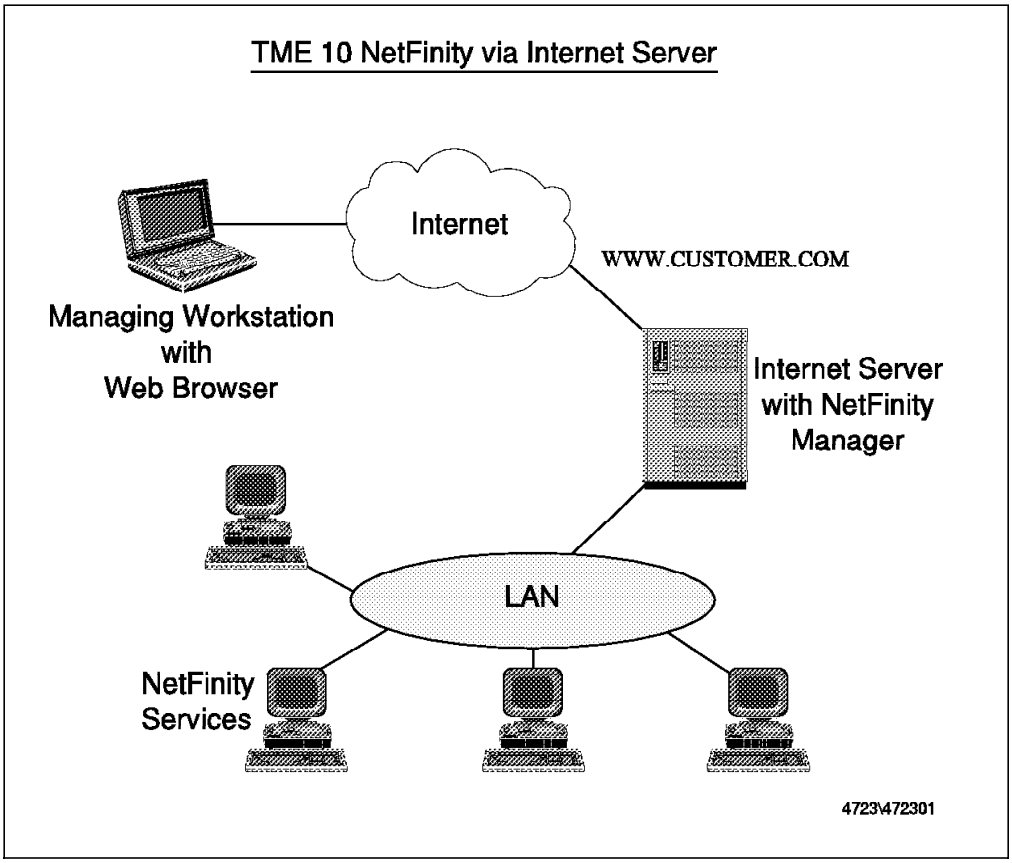


Figure 175. Connection Using Internet Server

A prerequisite for this solution is that you have a registered Internet server installed at your remote location.

On this Internet server the TME 10 NetFinity Manager code must also be installed to enable the access to the server using TME 10 NetFinity. You need to be aware of this fact, because it may reduce the number of possible Internet servers. Some operating systems are not supported by the TME 10 NetFinity Manager.

Because the logical address for this server is known in the Internet, you can access this server by its Internet address (for example, WWW.IBM.COM) or its Internet TCP/IP address. After accessing this Internet server you can use its TME 10 NetFinity manager function to access the other workstations in the remote LAN. In case you have a firewall installed in your Internet server, you are still able to access the TME 10 NetFinity Manager on the Internet server using the Internet. You are then able to access the LAN using TME 10 NetFinity. Always keep in mind, that you have to carefully configure the access rights to the manager code on the Internet server from the Web site. See 6.2, “Configuration of the Web Manager” on page 151 for details on the Web configuration, as well as configuring the access rights using the Security Manager of TME 10 NetFinity. You should always define the Web access to the

TME 10 NetFinity manager with dedicated TCP/IP addresses and not configure the access with any remote host access. This is very important, because if you don′t restrict this access, then you might compromise security and your LAN would be open to any Internet user, if this user has the TME 10 NetFinity code installed and got information about one of your TCP/IP addresses.

Of course you may also install the Internet server on a different system and then access a TME 10 NetFinity Manager which is physically installed on a different managing workstation within the LAN. The address of this managing workstation must now be known by the local TME 10 NetFinity manager, because this is now the location address, which he or she will access with TME 10 NetFinity Web Manager and *not* the location address of the Internet server. Normally you have a firewall installed to prevent your LAN from being accessed by a user from outside via the Internet. In this case you cannot access a workstation connecte to a remote LAN directly; the firewall omits this possibility.

See Figure 175 on page 147 for an overview of this connection. You will access this server or the TME 10 NetFinity managing workstation by its Internet address. Prerequisites on the remote location for this connection are the following:

1. All workstations have at least one supported network device driver installed.
2. All workstations connected to the remote LAN have at least the TME 10 NetFinity services installed.
3. One system, which is also connected to the remote LAN, has been configured as an Internet server with the appropriate Internet connections established.
4. The Internet server also has the TME 10 NetFinity Manager code installed or one of the workstations within the LAN has the manager code installed.
5. The NetFinity Manager on the Internet server or the TME 10 NetFinity managing workstation at the remote LAN has proper security configuration set up so that the local TME 10 NetFinity Manager is allowed to access this server. See 6.2, “Configuration of the Web Manager” on page 151 for details on this configuration.

6.1.2 Accessing Remote LANs Using a Service Provider

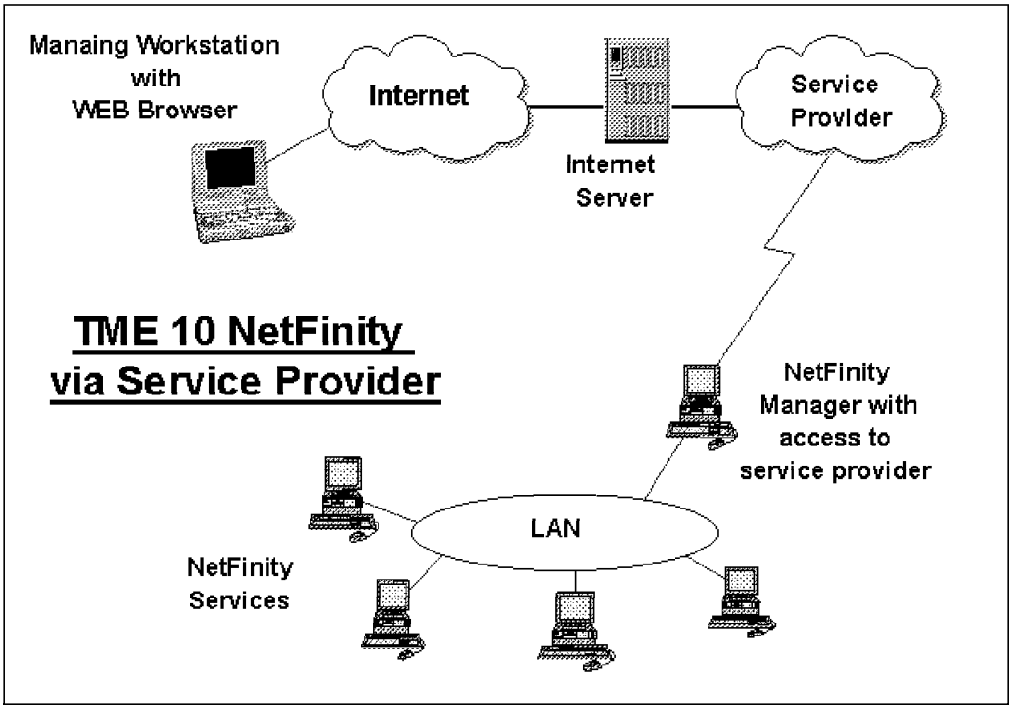


Figure 176. Connection Using Service Provider

The easiest way to use the Internet access facilities is to use an Internet service provider, for example, CompuServe. These service providers give you with an official Internet address for your workstation, which may be used to access your local managing workstation. See the information below for an explanation. You may get access to the Internet on either or both sites using a service provider. This means that you can define the access to the Internet using for example, CompuServe for the managing workstation as well as for the managed workstation.

1. All workstations have at least one supported network device driver installed.
2. All workstations connected to the remote LAN have the TME 10 NetFinity Services installed.
3. One system, which is also connected to the remote LAN, has been configured to access the service providers network (such as logging on to CompuServe) and activated the Internet access using this service provider.
4. The gateway system also has established the Internet connection through the service providers network. In some cases this workstation has to have a specific software configuration. The different service providers will give you the appropriate configuration details, which may also be different depending on the software product being used to connect to the service providers network.

   Please be aware that the Internet TCP/IP address provided by your service provider might change every time you log on to your service providers network. We experienced this symptom when for example, logging on to CompuServe and accessing the Internet using CompuServe. Every time we got a different TCP/IP address. There is a possibility to define a specific TCP/IP address for your connection to your service provider. This depends, of course, on your service provider. In some cases the service provider will

ask you to define a specific connection within your network for this access. This means, that you may have to install and define a gateway for this connection at a fixed phone number/connection and you might only be able to access this remote LAN using the service provider only through this defined connection. This might also gives you more security for your connection. Please check with your service provider on these details. For example, we checked with CompuServe to see if this is possible. CompuServe assured us that this is not a problem but you have to apply for this connection, which might not be free of charge.

5. The gateway workstation which is connected to the service providers network also has the TME 10 NetFinity manager code installed.
6. The TME 10 NetFinity manager at the Internet gateway workstation has proper security configuration set up, so that the local managing workstation is allowed to access this system. See 6.2, “Configuration of the Web Manager” on page 151 for details on how to set up the configuration.

6.1.3 Accessing Remote LANs Using an Internet TCP/IP Address

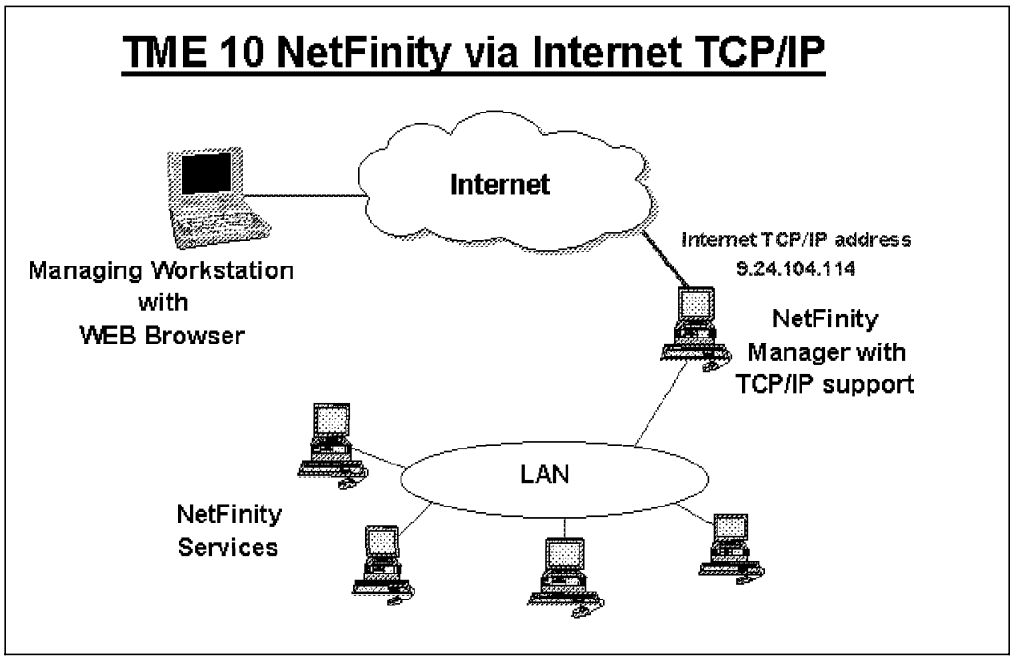


Figure 177. Connection Using Internet TCP/IP Address

A prerequisite for this way of accessing the remote site is that you have an Internet TCP/IP address available and configured for your managing workstation in the remote LAN. These TCP/IP addresses can be received from a service provider. This workstation has to have a way to be accessed over the Internet. You access this remote workstation and therefore the LAN behind it by using the TCP/IP address instead of accessing a WWW server name. There are some prerequisites which have to be solved, before monitoring the remote LAN:

1. All workstations have at least one supported network device driver installed.
2. All workstations connected to the remote LAN have at least the TME 10 NetFinity Services installed.
3. One system, which is also connected to the remote LAN, has been configured with an appropriate Internet TCP/IP address, which has been

provided by a service provider and the Internet connections have been established.

4. The gateway workstation to the Internet also has the TME 10 NetFinity Manager code installed.
5. The TME 10 NetFinity Manager at the Internet gateway workstation has the proper security configuration set up, so that the local managing workstation is allowed to access this system. See 6.2, “Configuration of the Web Manager” for details on how to set up the configuration.

6.2 Configuration of the Web Manager

Figure 178. Webability

On the gateway workstation of the remote location you have to set up some definitions so that you are able to connect to it using the Internet. You also want to set up some additional security, so that not everybody who establishes a connection to your Internet gateway also gets access to your TME 10 NetFinity functions on the gateway.

The Web access definition cannot be changed while accessing this gateway over the Internet. This means, that you can only change the Web access definitions for the gateway locally at the gateway workstation or from another TME 10 NetFinity Manager workstation, which is physically attached to the same LAN as the gateway. This gives you additional security, so that nobody can define additional access rights to your gateway using the Internet connection.

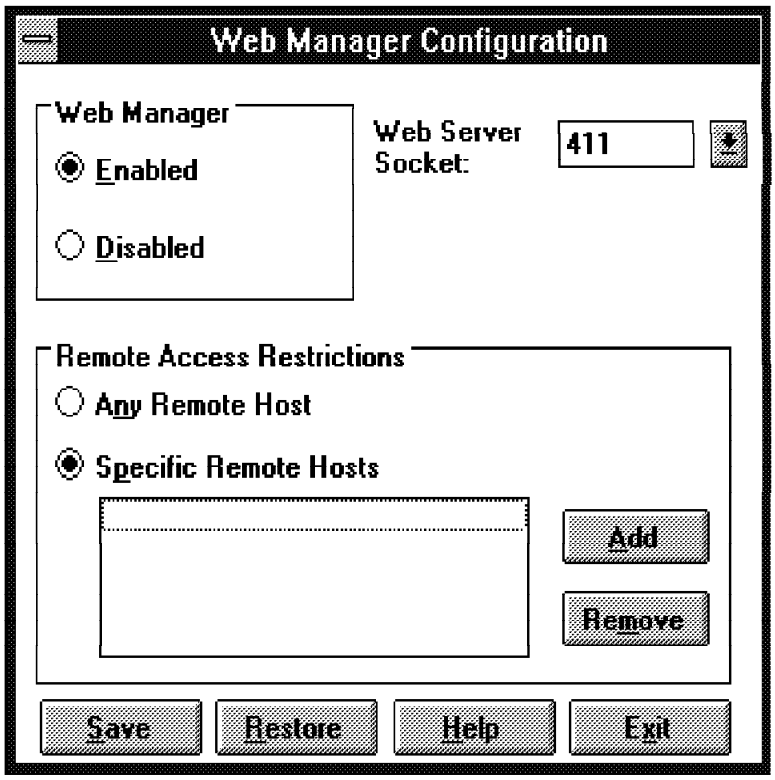


Figure 179. Web Manager Configuration

Figure 179 shows the definition screen for the Web access to your gateway. You at least have to enable the Web Manager and define a Web server socket.

- Web Manager defines the status of the Web access to your gateway with:
  - Enabled means that in general the access to your gateway from the Internet is enabled.
  - Disabled means that in general the access to your gateway from the Internet has been disabled and *no* TME 10 NetFinity Manager from outside your LAN is allowed to access this gateway from the Internet.
- Web Server Socket - In here you define the Web sockets, which are the TCP/IP sockets. In our case, logical connection definitions for the Internet access. Theoretically, this can be any numeric value, but the TME 10 NetFinity Manager that wants to access this gateway has to know this value. The default value is 411, but you can define any value (0 - 32767). Most Web servers use the socket number 80. This is the reason why TME 10 NetFinity Web manager by default gives you a value of 411. This is to reduce the chance of possible conflicts with your already existing Internet servers sockets. We see later in this chapter how it is used.
- Remote Access Restrictions - Defines who may access this gateway via the Internet. You should always define the Web access to the TME 10 NetFinity manager with dedicated TCP/IP addresses or address ranges and not configuring the access with any remote host access. This is very important, because if you don't restrict this access, then you could get around the security functions of the firewall and your LAN would be open to any Internet user, if this user has information about one of your TCP/IP addresses. Of course there are still the security functions of NetFinity, which prevent further access than the main menu of the gateway.

- Any Remote Host - Means, that anybody, who manages to get the connection to your gateway may access at least the main menu of the gateways TME 10 NetFinity Manager. How far these users can get then depends on the Security Managers definitions in the gateway or the managing workstation, which you should define very carefully. See also 2.1.1.5, “Security Manager” on page 20 for details on the Security Manager definitions.
- Specific Remote Hosts - In here you define which workstations may access this managing workstation using the Internet. See Figure 180 for definition details on this host definitions.

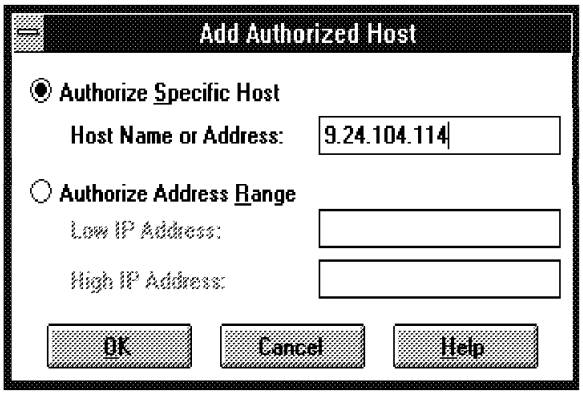


Figure 180. Host Access Definition

The Add Authorized Host menu gives you the possibility to allow and restrict access to the managing workstation from other TME 10 NetFinity managers using the Internet. But still the TME 10 NetFinity Security Manager restricts the access to the TME 10 NetFinity Managers Services at the gateway.

- Authorize Specific Host - Here you can define single TCP/IP addresses of workstations that might access your gateway and the main menu of your TME 10 NetFinity at the gateway. In our example we use a managing workstation that has a TCP/IP address of 9.24.104.114 defined. Only this one workstation is now able to access this gateway.
- Authorize Address Range - The same applies for this definition except that here you can define an address range for TME 10 NetFinity Managers, that may access this gateway using the Internet.

6.3 Internet Client Functions

This chapter describes the functionality and limitations when using the TME 10 NetFinity Manager and its Internet connection.

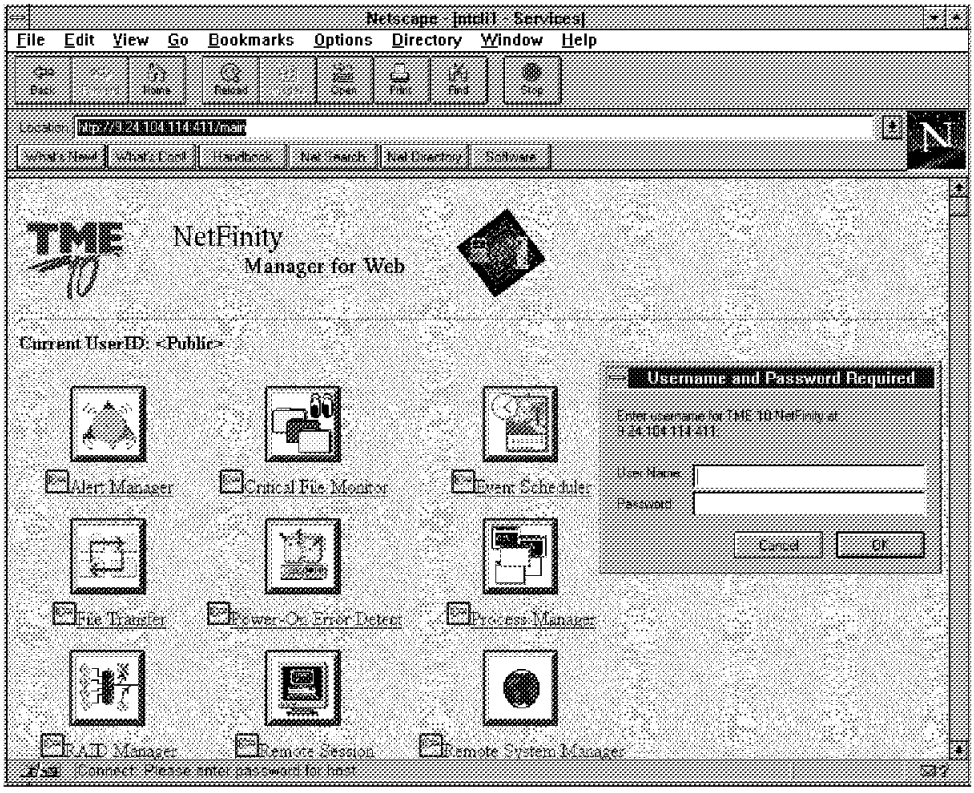


Figure 181. TME 10 NetFinity Main Menu

When you try to access a gateway from a TME 10 NetFinity managing workstation you first have to start a Web browser. In our example we use Netscape running under Windows NT 3.51 and under AIX. It should also soon be supported on OS/2. Of course, the same functions are also available using other Web browser software products like OS/2 WebExplorer. Each make of the Web browsers have slightly different functions, so you need to be aware of their capabilities. As the accessing location you have to define the gateways host name or the Internet address of the managing workstation at the remote LAN, depending on the type of Internet server you are using and how it is configured. This address may be a TCP/IP address or an Internet server host name. The following shows you some details for this configuration. In our first example, we accessed the gateway using a TCP/IP address. In our second example you can see the same access using host names. The results of both accesses would be the same.

```
HTTP://9.24.104.114:411/MAIN
              |         |    |
              |         |    NetFinity Main Menu
              |         |
              |    TCP/IP Socket
              |     on Gateway
              |
   TCP/IP address of
  Gateway workstation
```

Note

These are just examples that were suitable for our environment. The host name shown above and the TCP/IP address are not accessible from outside the IBM firewall. Also, the socket address of 411 is a default address that you can change when you configure the Webability function.

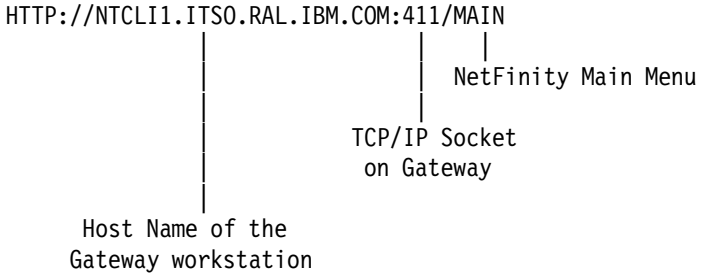


Figure 181 on page 154 shows you how to access the main menu at the gateways TME 10 NetFinity menu. If you are using the default socket *80*, then you may omit it, otherwise you have to give the correct socket number. Please be aware that your Web browser′s workstation TCP/IP address has to be given access to the gateway. This is done within the Web Manager configuration at the gateway. See 6.2, “Configuration of the Web Manager” on page 151 for details on how to configure it. If you now try to access one of the TME 10 NetFinity services and you now have set up the security manager in this gateway properly, you should receive a pop-up menu that requests that you enter a valid user ID and password. As you can see in the above picture, all of the TME 10 NetFinity services icons have a key symbol beside them. This means that these services are not available to public users. To use these services you have to enter the user ID and password that was defined in the TME 10 NetFinity security table. For those services that don′t have a key symbol beside them, you do not need a user ID to use them. If you now enter an invalid user ID or password then you will not be allowed to use the TME 10 NetFinity services of your gateway. On this main menu you can see that even using the Internet access to a workstation, you get the same icons for your TME 10 NetFinity services as you get from the regular desktop interface GUI. Therefore, from an operations perspective, there is very little new training that is required. There are just a few restrictions in using the different services with the Web browser. See 6.3.1, “Limitations When Using the Web Manager” on page 164 for details on these restrictions.

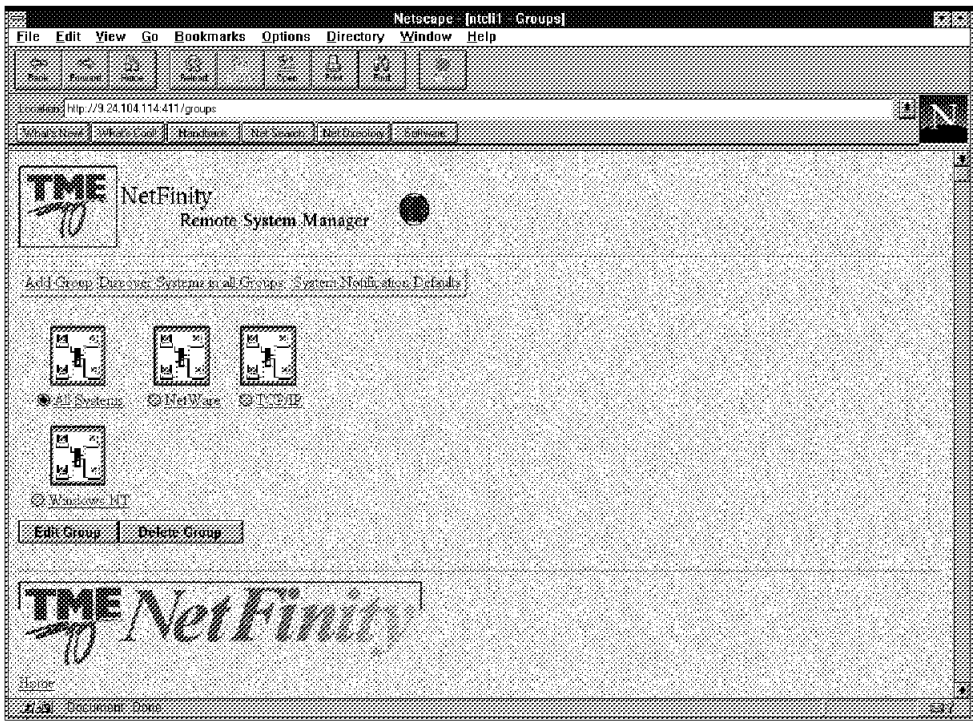


Figure 182. Remote System Manager

In our example we selected the Remote System Manager service, because we didn't want to monitor the gateway, but the workstations connected to the LAN. After selecting the Remote System Manager you get a list of already defined groups, which you also may edit the way you did when you were defining and editing groups locally.

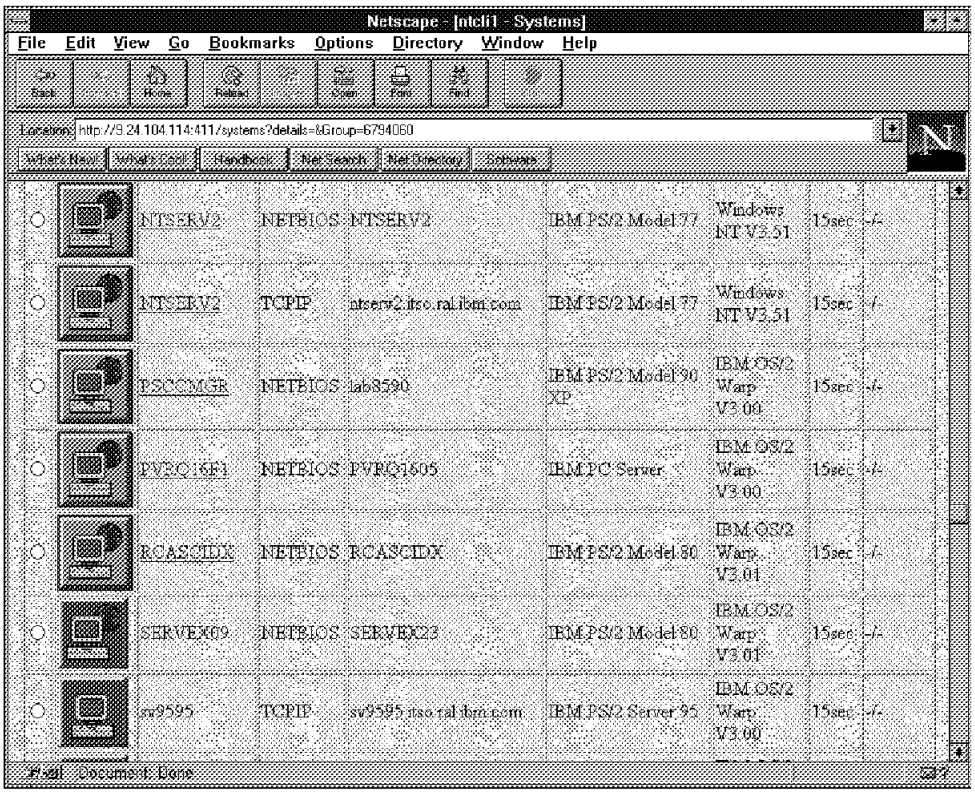

Netscape - [ntcli1 - Systems]
File Edit View Go Bookmarks Options Directory Window Help
Location: http://9.24.104.114:411/systems?details=&Group=6794060
What's New! What's Cool! Handbook Net Search Net Directory Software
NTSERV2 NETBIOS NTSERV2 IBM PS/2 Model 77 Windows NT V3.51 15sec -/-
NTSERV2 TCPIP ntserv2.itso.ral.ibm.com IBM PS/2 Model 77 Windows NT V3.51 15sec -/-
PSCCMGR NETBIOS lab8590 IBM PS/2 Model 90 XP IBM OS/2 Warp V3.00 15sec -/-
PVRQ16F1 NETBIOS PVRQ1605 IBM PC Server IBM OS/2 Warp V3.00 15sec -/-
RCASCIDX NETBIOS RCASCIDX IBM PS/2 Model 80 IBM OS/2 Warp V3.01 15sec -/-
SERVEX09 NETBIOS SERVEX23 IBM PS/2 Model 80 IBM OS/2 Warp V3.01 15sec -/-
sv9595 TCPIP sv9595.itso.ral.ibm.com IBM PS/2 Server 95 IBM OS/2 Warp V3.00 15sec -/-
Document Done

Figure 183. Group Details

If you now select a group, then you have the same display functions as you had with the regular TME 10 NetFinity interface. This means that you can view the groups either as an Icon View or with the Group Details View. With the Group Details menu shown in Figure 183 you can see one of the groups we defined in this managing workstation. From the background color of the workstations icon you can easily recognize the status of it. If its red, it means that it is offline and if it is green, then that workstation is online and accessible by a TME 10 NetFinity managing workstation. The information given by this menu is very similar to what you had with the TME 10 NetFinity desktop interface.

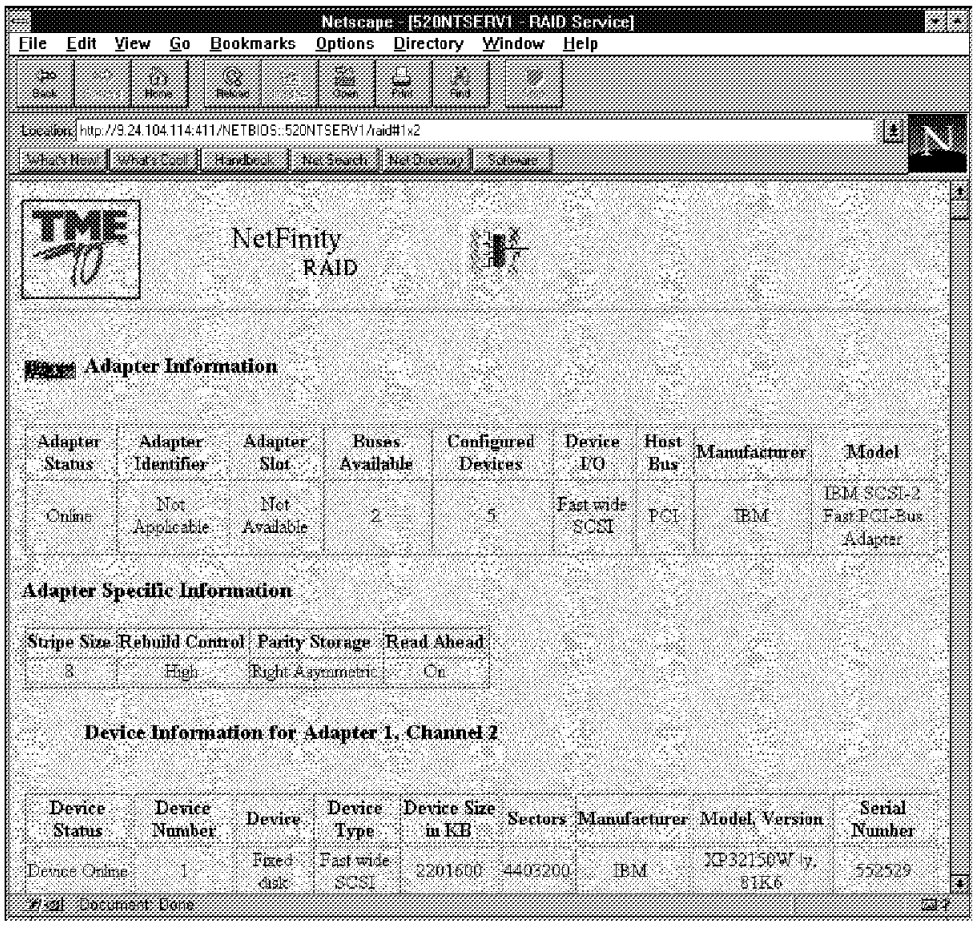

Netscape - [520NTSERV1 - RAID Service]
File Edit View Go Bookmarks Options Directory Window Help
Location: http://9.24.104.114:411/NETBIOS:.520NTSERV1/raid#1x2
What's New! What's Cool! Handbook Net Search Net Directory Software
TME 10
NetFinity
RAID
Adapter Information
Adapter Status | Adapter Identifier | Adapter Slot | Buses Available | Configured Devices | Device I/O | Host Bus | Manufacturer | Model
Online | Not Applicable | Not Available | 2 | 5 | Fast wide SCSI | PCI | IBM | IBM SCSI-2 Fast/PCI-Bus Adapter
Adapter Specific Information
Stripe Size | Rebuild Control | Parity Storage | Read Ahead
8 | High | Right Asymmetric | On
Device Information for Adapter 1, Channel 2
Device Status | Device Number | Device | Device Type | Device Size in KB | Sectors | Manufacturer | Model, Version | Serial Number
Device Online | 1 | Fixed disk | Fast wide SCSI | 2201600 | 4405200 | IBM | IC32150W v. 81K6 | 552529
Document: Done

Figure 184. RAID Information 1 of 2

In our example we selected an IBM PC Server 520 and then we selected the RAID Manager service. The information from this service can be seen in Figure 184 and Figure 185 on page 159. Using the Internet access to TME 10 NetFinity functions usually provides you with detailed information right away instead of forcing you to drill down through many menus to get to the information. This saves the company time and money. In this example using the RAID Manager service you can see that you get all the possible details about the RAID subsystem not in a graphical view, but more as a table of information, which is faster to access and display. In many cases, it is also easier to understand.

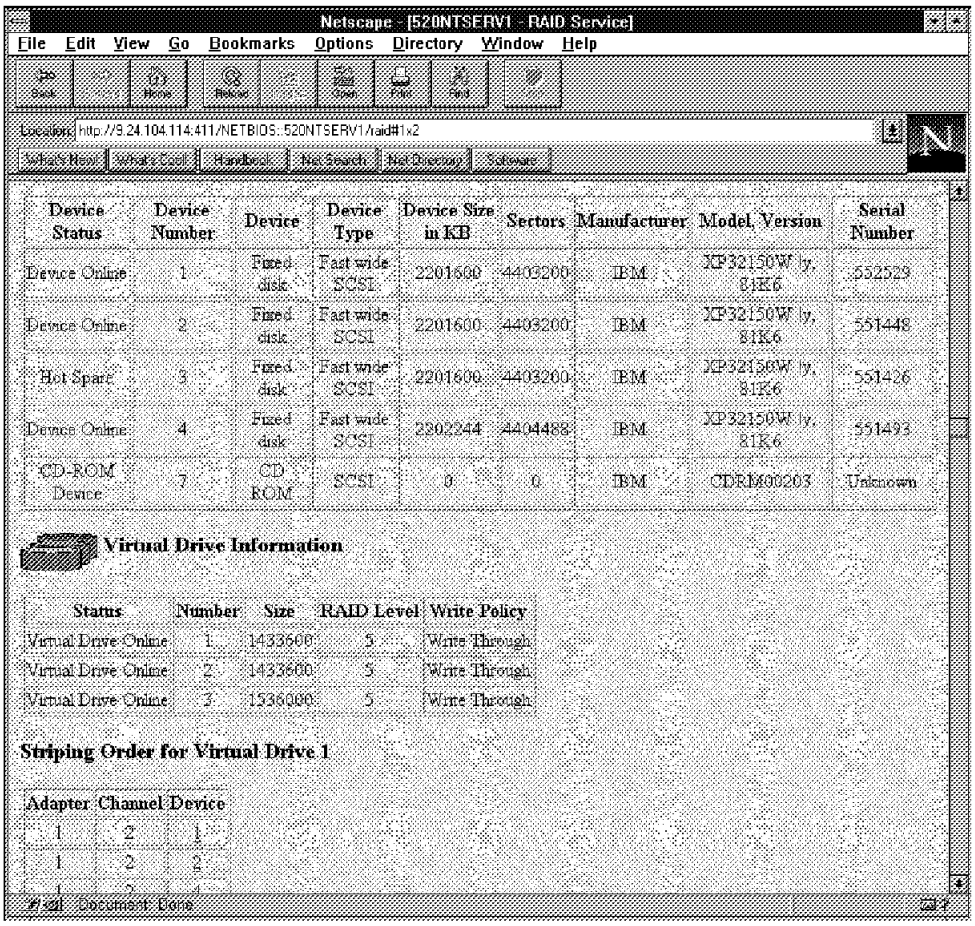

Netscape - [520NTSERV1 - RAID Service]
File Edit View Go Bookmarks Options Directory Window Help
Location: http://9.24.104.114.411/NETBIOS: 520NTSERV1/raid#1x2
What's New! What's Cool! Handbook Net Search Net Directory Software
Device Status | Device Number | Device | Device Type | Device Size in KB | Sectors | Manufacturer | Model, Version | Serial Number
Device Online | 1 | Fixed disk | Fast wide SCSI | 2201600 | 4403200 | IBM | XP32150W ly, 81K6 | 552529
Device Online | 2 | Fixed disk | Fast wide SCSI | 2201600 | 4403200 | IBM | XP32150W ly, 81K6 | 551448
Hot Spare | 3 | Fixed disk | Fast wide SCSI | 2201600 | 4403200 | IBM | XP32150W ly, 81K6 | 551426
Device Online | 4 | Fixed disk | Fast wide SCSI | 2202244 | 4404488 | IBM | XP32150W ly, 81K6 | 551493
CD-ROM Device | 7 | CD ROM | SCSI | 0 | 0 | IBM | CDRM00203 | Unknown
Virtual Drive Information
Status | Number | Size | RAID Level | Write Policy
Virtual Drive Online | 1 | 1433600 | 5 | Write Through
Virtual Drive Online | 2 | 1433600 | 5 | Write Through
Virtual Drive Online | 3 | 1536000 | 5 | Write Through
Striping Order for Virtual Drive 1
Adapter | Channel | Device
1 | 2 | 1
1 | 2 | 2
Document Done

Figure 185. RAID Information 2 of 2

There are also some differences with the other TME 10 NetFinity services via the Internet. Following you will see two menus that show the some of the information that you get from the System Information service. In Figure 186 on page 160 you can see the overview of the information available for the system information. Next select one of the functions such as Adapter Information. If you select one of the functions, you will go directly to the requested information. See for example, Figure 187 on page 160 for adapter detail information. You may also scroll down the screen and you will see all the possible information from the system information service directly after the icon view. This means that in most cases the detailed information from the different services is already available when you see the overview screen of each function.

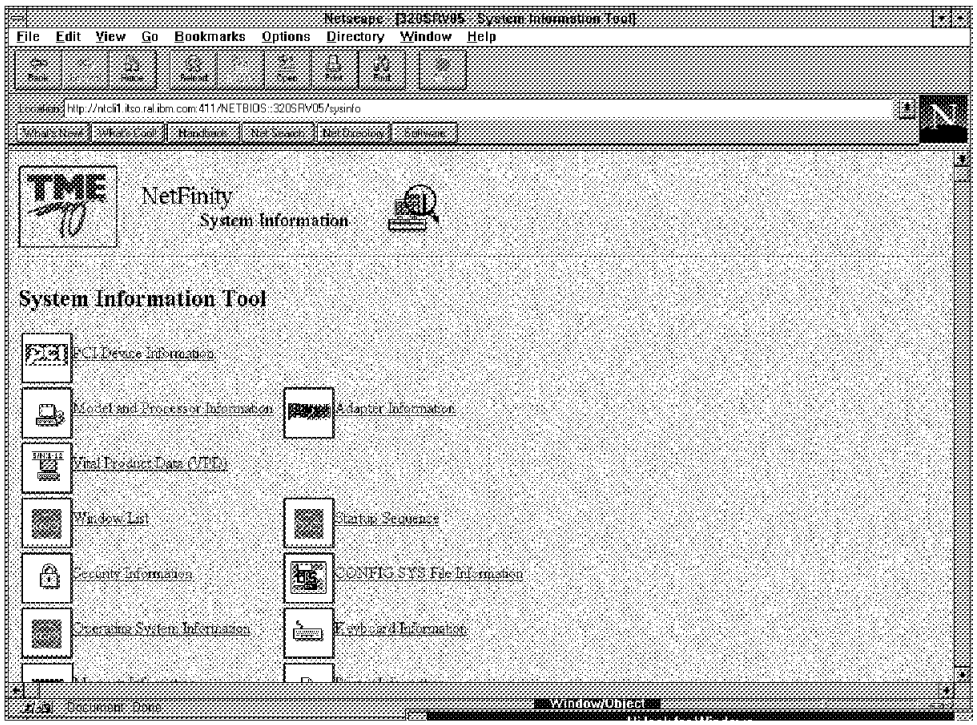


Figure 186. System Information Icons

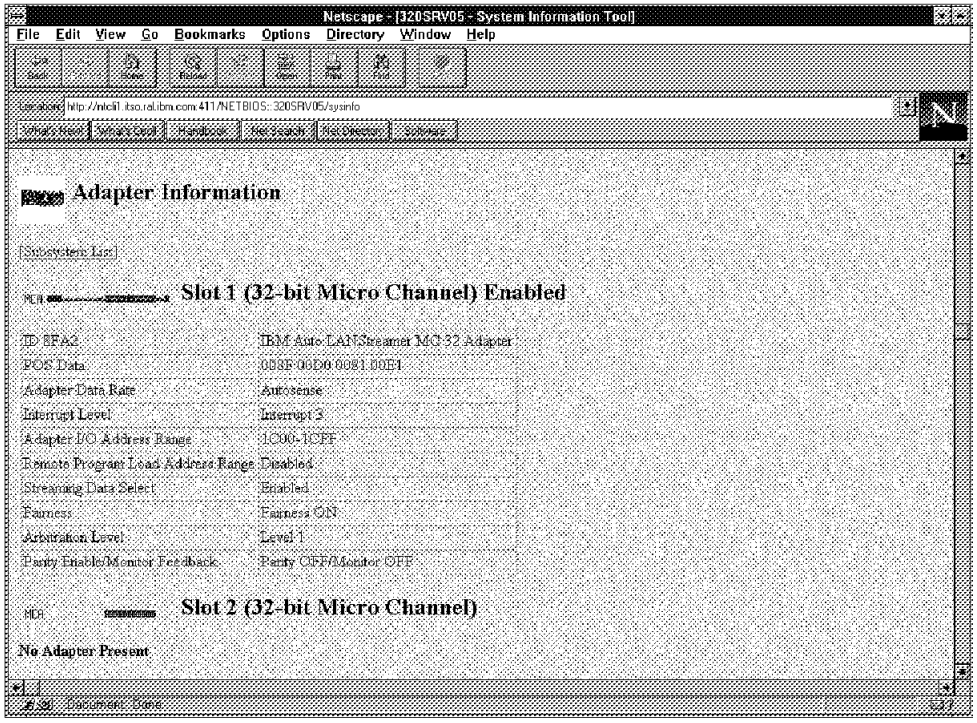

Netscape - [320SRV05 - System Information Tool]
File Edit View Go Bookmarks Options Directory Window Help
Adapter Information
[Subsystem List]
Slot 1 (32-bit Micro Channel) Enabled
ID 8FA2 IBM Auto LANStreamer MC 32 Adapter
POS Data 0BBF 00D0 0081 00E1
Adapter Data Rate Autosense
Interrupt Level Interrupt 3
Adapter I/O Address Range 1C00-1CFF
Remote Program Load Address Range Disabled
Streaming Data Select Enabled
Fairness Fairness ON
Arbitration Level Level 1
Parity Enable/Monitor Feedback Parity OFF/Monitor OFF
Slot 2 (32-bit Micro Channel)
No Adapter Present

Figure 187. System Information Details

Another example of how the TME 10 NetFinity services look when using the Web interface is the following. We were using the event scheduler to schedule the usage of the system information service.

Figure 188. Event Scheduler Definition 1 of 3

It is very easy to use the event scheduler function using the Web service, because you don't have to go through several different definition menus; you get all the required definitions in one. Figure 188 through Figure 190 on page 163 shows the configuration menus for this function.

Figure 189. Event Scheduler Definition 2 of 3

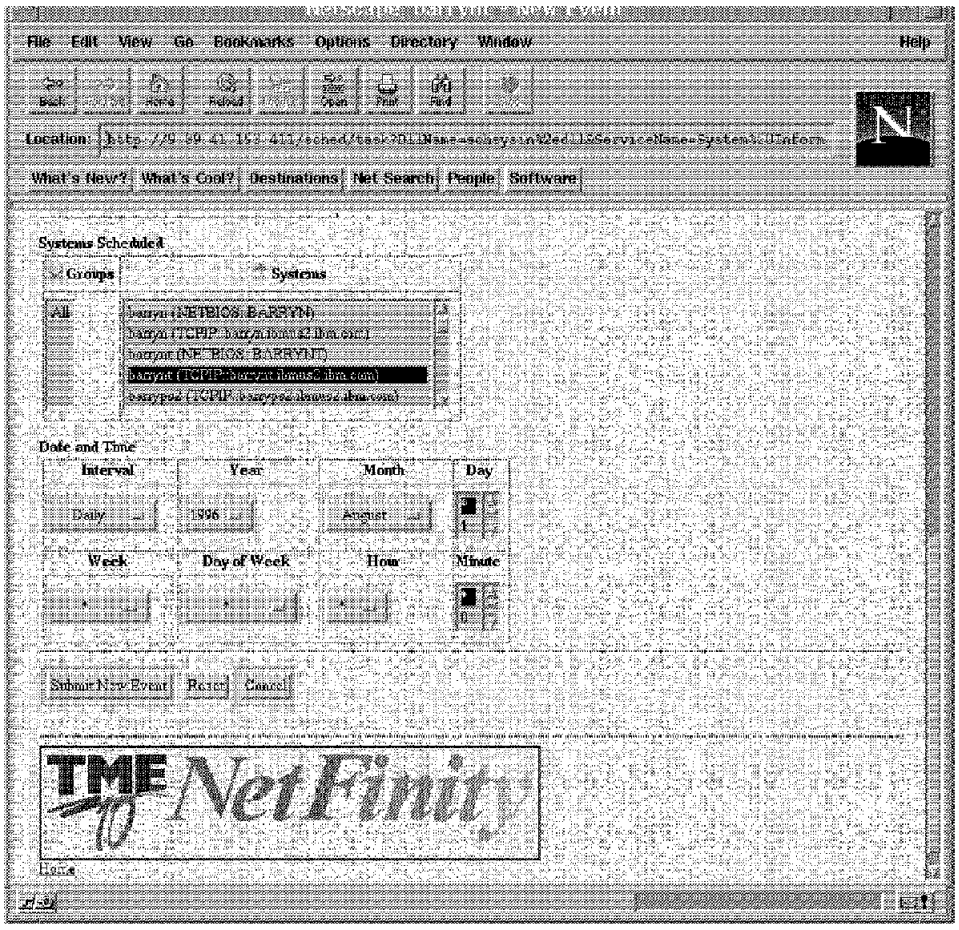


Figure 190. Event Scheduler Definition 3 of 3

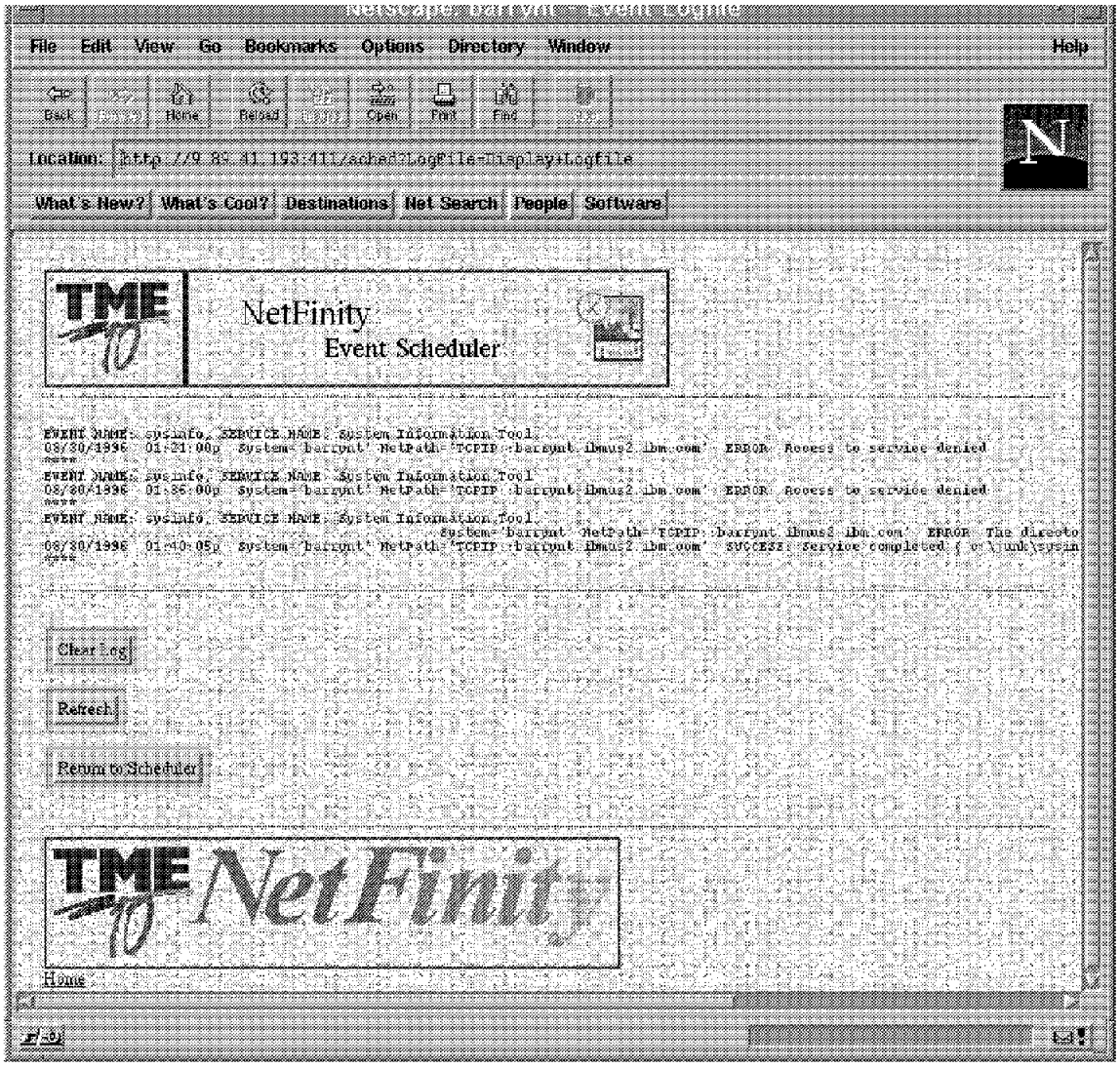

File Edit View Go Bookmarks Options Directory Window Help
Back Forward Home Reload Images Open Print Find Stop
Location: http://9.85.41.193:411/sched?LogFile=display+Logfile
What's New? What's Cool? Destinations Net Search People Software
TME 10
NetFinity
Event Scheduler
EVENT NAME: sysinfo, SERVICE NAME: System Information Tool
08/30/1996 01:21:00p system='barrynt' NetPath='TCPIP :barrynt.ibmus2.ibm.com' ERROR Access to service denied
EVENT NAME: sysinfo, SERVICE NAME: System Information Tool
08/30/1996 01:36:00p system='barrynt' NetPath='TCPIP :barrynt.ibmus2.ibm.com' ERROR Access to service denied
EVENT NAME: sysinfo, SERVICE NAME: System Information Tool
system='barrynt' NetPath='TCPIP :barrynt.ibmus2.ibm.com' ERROR The directo
08/30/1996 01:40:05p system='barrynt' NetPath='TCPIP :barrynt.ibmus2.ibm.com' SUCCESS service completed (c:\junk\systm
Clear Log
Refresh
Return to Scheduler
TME 10 NetFinity
Home

Figure 191. Event Scheduler Results

Note

The failures in the scheduled activities were due to the fact that the public user ID did not have access to the *sysinfo* service. After updating the security information, we successfully ran the service, using the scheduler function.

6.3.1 Limitations When Using the Web Manager

There are a few limitations if you will be using the TME 10 NetFinity Manager with a Web browser. In this chapter we show you these restrictions and requirements.

1. The Web browser that is used has to support Hypertext Markup Language (HTML) 2.0 or higher (such as IBM OS/2 WebExplorer). Most of the browsers on the market meet this requirement.
2. The TME 10 NetFinity Remote Session service can only be used by a browser that supports the Java programming language (for example, Netscape Navigator).

3. Be careful that you are not defining a TCP/IP socket number that is already used by another Internet server.
4. When accessing a workstation with the Web manager, you will see all available TME 10 NetFinity services on the remote workstation, but some of them might not be available to you. This is different from a connection using a local LAN protocol, where you only receive the icons for the services for which you have access.
5. Some Web browsers keeping the Web pages in memory and in cache, so that if you are recalling the same page once again, then the values shown in the browser may not be the actual values. Instead you will see old values from the stored Web page. If you are using this kind of a Web browser, then you should always reload the pages. See your Web browsers documentation for its description.
6. The DMI-browser is not available when using the Web manager.
7. The System Partition is also not available when using the Web manager service. If you are using the System Partition Access using the Event Scheduler Service, then you will have this service available, but you cannot directly use it without the Event Scheduler service.
8. There are no help menus available within the Web manager since some of the Web browsers don't support functions such as context menus.
9. Those functions that are normally used using an objects context menu are available using radio buttons within the different Web managers menus.
10. All database export features within the Alert Manager, Event Scheduler, Software Inventory, System Information Tool, System Monitor and System Profile are not available, when accessing a system using the Web manager.
11. When using the Screen View Service using the Web manager the screen contents are not saved as a bit map, but as a JPEG format picture.
12. The Monitor Service does not give you the ability to display the monitored resources in a graphic format, but only in a numeric representation. This value is not automatically refreshed. You will first see the values for all resources, then you may select some or all of the resources and define a refresh cycle in number of seconds. This reduces excessive network load.

Appendix A. Application Alerts and Alert IDs

Table 2 (Page 1 of 2). TME 10 NetFinity Alerts

Application	**Application ID**		
Alert	Alert Type	Severity *	Application Alert Type
Security Manager	**SecMgr**		
Access Granted	Securitiy Information	7	20
Public Access Granted	Securitiy Information	6	21
System Access Denied	Security Warning	5	22
System Restart Initiated	Security Information	5	41
System Restart Request Rejected	Security Error	3	40
System Monitor Service	**MonitorB**		
Upper Range Threshold Error	Error	x	0000
Upper Range Threshold Warning	Warning	x	0000
Lower Range Threshold Warning	Warning	x	0000
Lower Range Threshold Error	Error	x	0000
Threshold Return to Normal	Warning	x	10
Physical RAID Device Online	Information	3	130
Physical RAID Device Standby	Error	2	130
Physical RAID Device Dead	Failure	0	130
Logical RAID Device Online	Information	3	131
Logical RAID Device Critical	Error	2	131
Logical RAID Device Offline	Failure	0	131
Power-On Error Detect	**POED**		
Power-On Error Detect	Application Failure	4	0201
Predictive Failure Analysis	**PFA**		
Predictive Failure	Disk Failure	x	0000
Critical File Monitor	**MonCritF**		
File Changed	Warning	x	0
File Deleted	Warning	x	1
File Created	Warning	x	2
Process Manager	**ProcMgr**		

© Copyright IBM Corp. 1996

Table 2 (Page 2 of 2). TME 10 NetFinity Alerts			
Process Terminated	Application Information	x	0901
Process Started	Application Information	x	0900
Process Failed to Start	Application Information	x	0902
Remote System Manager	**NetMgr**		
System Online Notification	System Information	x	000A
System Offline Notification	System Information	x	000B
Service Manager	**SvcMgr**		
Service Start Request	Security Information	7	0900
Service Start Request Rejected	Security Warning	5	0901
* x = can be defined in the range 0 to 7			

Appendix B. List of Supported Modems

Table 3 (Page 1 of 2). Supported Modems for TME 10 NetFinity

Manufacturer	**Type/Model**
Aspen	14.4IFX 28.8IFX 14.4EFX 28.8EFX
Bocamodem	MV.34I MV.34E M144AE
Cardinal	MVP288XF
Hayes	ACCURA 96+FAX96 ACCURA 96B+FAX96 ACCURA 144+FAX144 ACCURA 144B+FAX144 ACCURA 288V.FC+FAX OPTIMA 96+FAX96 OPTIMA 96B+FAX96 OPTIMA 144+FAX144 OPTIMA 144B+FAX144 OPTIMA 288V.34/V.FC+FAX OPTIMA 288BV.34/V.FC+FAX
IBM	7855-10 7852-10 Mwave 14.400
Maxtech	14.4 Kbps FAX Modem Series 14.4 Kbps Voice/FAX Modem 28.8 Kbps FAX Modem Series F-1114PV1 PCMCIA VF-1114PV1 PCMCIA
Megahertz	CC3144 CC3288 CC4144 P2144 XJ1144 XJ2288 XJ2144
Microcom	DeskPorte 14.4 DeskPorte 28.8S
Motorola	LifeStyle 28.8
Multimodem	MT1432ZDX MT1432ZDXI MT1432ZDXK MT1932ZDX MT1932ZDXK MT1932ZDXI MT2834ZDXI MT2834ZDXK MT2834ZDX PC144MT

© Copyright IBM Corp. 1996

Table 3 (Page 2 of 2). Supported Modems for TME 10 NetFinity	
Manufacturer	**Type/Model**
Practical Peripherals	PC144T2 PC144T2-EZ PM14400FXMT PM288MT II V.34
USRobotics	Sportster 14,400 FAX Modem Sportster 28,800 FAX Modem
VIVA	14.4
Zoom	14400 FaxModem

Appendix C. TME 10 NetFinity Monitors

Here is the list of NetFinity monitors for Version 4.0 plus NetFinity Partners monitors:

C.1 OS/2 System Monitors

```
CPU Utilization
Process Count
Thread Count
Pentium Processor
        Integer Instruction Rate
        Floating Point Instruction Rate
        Interrupt Rate
        Port I/O Rate
        Memory I/O Rate
        CPU Cache Hit Rate
Drive Space Used
Drive Space Remaining
Disk Work Load
Disk Error Rate
Print Jobs in Queue
OS/2 LAN Server Monitors
        Sessions
        Connections
        Opens
        Shares
        Bytes Sent
        Bytes Received
        Response Time
        Request Buf Shortage
        Big Buf Shortage
Locked Memory
Memory Usage
ECC Memory Errors
Swap File Size
Swap File Space Remaining
RAID Subsystem Status
```

C.2 Windows NT Monitors

```
CPU Utilization
Drive Space Used
Drive Space Remaining
Disk Workload
Locked Memory
Memory Usage
NT Server
        Sessions
        Opens
        Bytes Sent
        Bytes Received
TCP/IP Statistics
        UDP Datagrams Sent
        UDP Datagrams Received
        IP Packets Sent
```

© Copyright IBM Corp. 1996

IP Packets Received
IP Packets with Errors
TCP Connections
Unicast Packets Sent
Broadcast Packets Sent
Unicast Packets Received
Broadcast Packets Received
Bytes Sent
Bytes Received

C.3 NetWare 3.x/4.x Monitors

CPU Utilization
Cache Blocks in Use
Percent of Cache in Use
Process Count
Thread Count
Volume Space Used
Volume Spaced Remaining
Connected Users

C.4 Windows 3.x and Windows 95 Monitors

CPU Utilization
Disk Space Used
Disk Space Remaining
Memory Usage
Locked Memory
Windows Resources
Disk Workload

C.5 Monitors Provided by NetFinity Partners

C.5.1 APC (American Power Conversion)

OS/2 and NetWare

- UPS Run Time Remaining
- UPS Voltage
- UPS Battery Capacity
- UPS Load
- UPS Temperature
- UPS Humidity

C.5.2 Lexmark International

OS/2

- Pages printed per minute
- Pages in print queue

C.5.3 BMC Software

```
NetWare
Connections
     *Current Stations
     *Peak Stations
     *Maximum Stations (static)

Disk
     Disk Reads/Min
     Disk Writes/Min
     KBs Read/Min
     KBs Written/Min
     *Dirty Cache Buffers
     *Pending Write Requests

File System
     File Opens/Min
     File Creates/Min
     File Renames/Min
     File Deletes/Min
     Directory Searches/Min
     File Reads/Min
     File Writes/Min
     File KBs Read/Min
     File KBs Written/Min
     FAT Sectors Dirty/Min
     FAT Sectors Written/Min
     Record Locks/Min
     Transactions/Min

Memory
     *Original Cache Buffers (static)
     *Current Cache Buffers
     *Packet Receive Buffers
     *Directory Cache Buffers
     *Permanent Memory
     *Alloc Memory
     *Cache Memory
     *Movable Memory
     *NonMovable Memory

Miscellaneous
     *Service Processes
     *Files Open
Network

     Packets Received/Min
     Packets transmitted/Min
     KBs Received/Min
     KBs Transmitted/Min
     Packets Routed/Min

Processor
     Monitor Utilization (as computed by MONITOR.NLM)
     *CPU Speed (static)

SmartTune
     *MaxConnDiskWrites
     *DirtyDiskDelay
```

```
      *DirtyDirDelay
      *MaxConnDirWrites
      *MaxDirCacheBuffers
      *MinDirCacheBuffers
      *MaxRecvBuffers
      *MaxServProcs

LAN Adapters
      Total Packets Sent/Min
      Total Packets Received/Min
      *No ECB Available Count/Min
      *Send Packet Too Big Count/Min
      *Send Packet Too Small Count/Min
      *Receive Packet Overflow Count/Min
      *Receive Packet Too Big Count/Min
      *Receive Packet Too Small Count/Min
      *Send Packet Miscellaneous Errors/Min
      *Receive Packet Miscellaneous Errors/Min
      *Send Packet Retry Count/Min
      *Checksum Errors/Min
      *Hardware Receive Mismatch Count/Min
```

Appendix D. Special Notices

This publication is intended to help technical support personnel implement systems management using NetFinity V4.0 on the NT platform. In addition, it will help show how to use other built-in systems management functions. The information in this publication is not intended as the specification of any programming interfaces that are provided by TME 10 NetFinity. See the PUBLICATIONS section of the IBM Programming Announcement for NetFinity for more information about what publications are considered to be product documentation.

References in this publication to IBM products, programs or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM′s product, program, or service may be used. Any functionally equivalent program that does not infringe any of IBM′s intellectual property rights may be used instead of the IBM product, program or service.

Information in this book was developed in conjunction with use of the equipment specified, and is limited in application to those specific hardware and software products and levels.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to the IBM Director of Licensing, IBM Corporation, 500 Columbus Avenue, Thornwood, NY 10594 USA.

The information contained in this document has not been submitted to any formal IBM test and is distributed AS IS. The information about non-IBM (″vendor″) products in this manual has been supplied by the vendor and IBM assumes no responsibility for its accuracy or completeness. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer′s ability to evaluate and integrate them into the customer′s operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk.

Any performance data contained in this document was determined in a controlled environment, and therefore, the results that may be obtained in other operating environments may vary significantly. Users of this document should verify the applicable data for their specific environment.

Reference to PTF numbers that have not been released through the normal distribution process does not imply general availability. The purpose of including these reference numbers is to alert IBM customers to specific information relative to the implementation of the PTF when it becomes available to each customer according to the normal IBM PTF distribution process.

The following terms are trademarks of the International Business Machines Corporation in the United States and/or other countries:

AIX	AT
Client Access	Current

© Copyright IBM Corp. 1996

DB2	FFST/2
IBM	Micro Channel
Mwave	NetFinity
NetView	OS/2
OS/400	PowerPC
Predictive Failure Analysis	SystemView
WebExplorer	XGA
400	

The following terms are trademarks of other companies:

C-bus is a trademark of Corollary, Inc.

PC Direct is a trademark of Ziff Communications Company and is used by IBM Corporation under license.

UNIX is a registered trademark in the United States and other countries licensed exclusively through X/Open Company Limited.

Microsoft, Windows, and the Windows 95 logo are trademarks or registered trademarks of Microsoft Corporation.

APC	APC
CompuServe	CompuServe Incorporated and H&R Block, Incorporated
Dr. Watson	CompuServe Incorporated or Empirical Tools and Technology
Hayes	Hayes Microcomputer Products, Incorporated
IPX, NetWare, Novell	Novell, Incorporated
Java, Sun	Sun Microsystems, Incorporated
Lexmark	Lexmark International, Incorporated
Lotus Notes	Lotus Development Corporation
Megahertz	US Robotics Mobile Communications Corporation
Microcom	Microcom Systems, Incorporated
Motorola	Motorola, Incorporated
MS, MS-DOS, Windows NT	Microsoft Corporation
MT	NEC Technologies, Incorporated
Multimodem	Multi-Tech Systems, Incorporated
Netscape	Netscape Communications Corporation
Pentium, 80386	Intel Corporation
SAM	Symantec Corporation
SCSI	Security Control Systems, Incorporated
Sportster	U.S. Robotics
TME, TME 10	Tivoli Systems Inc., an IBM Company
USRobotics	U.S. Robotics

Other trademarks are trademarks of their respective companies.

Appendix E. Related Publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this redbook.

E.1 International Technical Support Organization Publications

For information on ordering these ITSO publications see “How To Get ITSO Redbooks” on page 179.

- *LAN Management Processes Using NetFinity*, SG24-4517
- *Workgroup Management Using SystemView for OS/2*, SG24-2596

A complete list of International Technical Support Organization publications, known as redbooks, with a brief description of each, may be found in:

International Technical Support Organization Bibliography of Redbooks, GG24-3070.

E.2 Redbooks on CD-ROMs

Redbooks are also available on CD-ROMs. **Order a subscription** and receive updates 2-4 times a year at significant savings.

CD-ROM Title	Subscription Number	Collection Kit Number
System/390 Redbooks Collection	SBOF-7201	SK2T-2177
Networking and Systems Management Redbooks Collection	SBOF-7370	SK2T-6022
Transaction Processing and Data Management Redbook	SBOF-7240	SK2T-8038
AS/400 Redbooks Collection	SBOF-7270	SK2T-2849
RISC System/6000 Redbooks Collection (HTML, BkMgr)	SBOF-7230	SK2T-8040
RISC System/6000 Redbooks Collection (PostScript)	SBOF-7205	SK2T-8041
Application Development Redbooks Collection (available soon)	SBOF-7290	SK2T-8037
Personal Systems Redbooks Collection (available soon)	SBOF-7250	SK2T-8042

E.3 Other Publications

These publications are also relevant as further information sources.

- *TME 10 NetFinity*, G325-6516
- *DB2 for Windows 95 & Windows NT V2R1.1 Planning Guide*, S33H-0314
- *Mastering Windows NT Server 3.51 - Second Edition*, SR28-5688-01

© Copyright IBM Corp. 1996

How To Get ITSO Redbooks

This section explains how both customers and IBM employees can find out about ITSO redbooks, CD-ROMs, workshops, and residencies. A form for ordering books and CD-ROMs is also provided.

This information was current at the time of publication, but is continually subject to change. The latest information may be found at URL http://www.redbooks.ibm.com.

How IBM Employees Can Get ITSO Redbooks

Employees may request ITSO deliverables (redbooks, BookManager BOOKs, and CD-ROMs) and information about redbooks, workshops, and residencies in the following ways:

- **PUBORDER** — to order hardcopies in United States
- **GOPHER link to the Internet** - type GOPHER.WTSCPOK.ITSO.IBM.COM
- **Tools disks**

  To get LIST3820s of redbooks, type one of the following commands:

  ```
  TOOLS SENDTO EHONE4 TOOLS2 REDPRINT GET SG24xxxx PACKAGE
  TOOLS SENDTO CANVM2 TOOLS REDPRINT GET SG24xxxx PACKAGE (Canadian users only)
  ```

  To get lists of redbooks:

  ```
  TOOLS SENDTO WTSCPOK TOOLS REDBOOKS GET REDBOOKS CATALOG
  TOOLS SENDTO USDIST MKTTOOLS MKTTOOLS GET ITSOCAT TXT
  TOOLS SENDTO USDIST MKTTOOLS MKTTOOLS GET LISTSERV PACKAGE
  ```

  To register for information on workshops, residencies, and redbooks:

  ```
  TOOLS SENDTO WTSCPOK TOOLS ZDISK GET ITSOREGI 1996
  ```

  For a list of product area specialists in the ITSO:

  ```
  TOOLS SENDTO WTSCPOK TOOLS ZDISK GET ORGCARD PACKAGE
  ```

- **Redbooks Home Page on the World Wide Web**

  http://w3.itso.ibm.com/redbooks

- **IBM Direct Publications Catalog on the World Wide Web**

  http://www.elink.ibmlink.ibm.com/pbl/pbl

  IBM employees may obtain LIST3820s of redbooks from this page.

- **ITSO4USA category on INEWS**
- **Online** — send orders to: USIB6FPL at IBMMAIL or DKIBMBSH at IBMMAIL
- **Internet Listserver**

  With an Internet E-mail address, anyone can subscribe to an IBM Announcement Listserver. To initiate the service, send an E-mail note to announce@webster.ibmlink.ibm.com with the keyword subscribe in the body of the note (leave the subject line blank). A category form and detailed instructions will be sent to you.

© Copyright IBM Corp. 1996

How Customers Can Get ITSO Redbooks

Customers may request ITSO deliverables (redbooks, BookManager BOOKs, and CD-ROMs) and information about redbooks, workshops, and residencies in the following ways:

- **Online Orders** (Do not send credit card information over the Internet) — send orders to:

	IBMMAIL	**Internet**
In United States:	usib6fpl at ibmmail	usib6fpl@ibmmail.com
In Canada:	caibmbkz at ibmmail	lmannix@vnet.ibm.com
Outside North America:	bookshop at dkibmbsh at ibmmail	bookshop@dk.ibm.com

- **Telephone orders**

United States (toll free)	1-800-879-2755
Canada (toll free)	1-800-IBM-4YOU
Outside North America	(long distance charges apply)
(+45) 4810-1320 - Danish	(+45) 4810-1020 - German
(+45) 4810-1420 - Dutch	(+45) 4810-1620 - Italian
(+45) 4810-1540 - English	(+45) 4810-1270 - Norwegian
(+45) 4810-1670 - Finnish	(+45) 4810-1120 - Spanish
(+45) 4810-1220 - French	(+45) 4810-1170 - Swedish

- **Mail Orders** — send orders to:

IBM Publications	IBM Publications	IBM Direct Services
Publications Customer Support	144-4th Avenue, S.W.	Sortemosevej 21
P.O. Box 29570	Calgary, Alberta T2P 3N5	DK-3450 Allerød
Raleigh, NC 27626-0570	Canada	Denmark
USA		

- **Fax** — send orders to:

United States (toll free)	1-800-445-9269
Canada	1-403-267-4455
Outside North America	(+45) 48 14 2207 (long distance charge)

- **1-800-IBM-4FAX (United States)** or **(+1) 415 855 43 29 (Outside USA)** — ask for:

  Index # 4421 Abstracts of new redbooks
  Index # 4422 IBM redbooks
  Index # 4420 Redbooks for last six months

- **Direct Services** - send note to softwareshop@vnet.ibm.com
- **On the World Wide Web**

Redbooks Home Page	http://www.redbooks.ibm.com
IBM Direct Publications Catalog	http://www.elink.ibmlink.ibm.com/pbl/pbl

- **Internet Listserver**

  With an Internet E-mail address, anyone can subscribe to an IBM Announcement Listserver. To initiate the service, send an E-mail note to announce@webster.ibmlink.ibm.com with the keyword subscribe in the body of the note (leave the subject line blank).

IBM Redbook Order Form

Please send me the following:

Title	Order Number	Quantity

- **Please put me on the mailing list for updated versions of the IBM Redbook Catalog.**

First name Last name

Company

Address

City Postal code Country

Telephone number Telefax number VAT number

- Invoice to customer number

- Credit card number

Credit card expiration date Card issued to Signature

We accept American Express, Diners, Eurocard, Master Card, and Visa. Payment by credit card not available in all countries. Signature mandatory for credit card payment.

DO NOT SEND CREDIT CARD INFORMATION OVER THE INTERNET.

Index

A
active client 5
Adapter Details 13
Alert
  Actions 31
  Definitions 31
  Logs 33
  Process Alerts 35
Alert Manager 30, 31
Alerts 29

B
bibliography 177

C
Clients
  active 5
  Passive 4
  Standalone 4
COM port 38
CompuServe 149
Configuration 7, 117, 152
Connections 2, 145, 146, 150
Critical File Monitoring 28

D
Database 45
Database Export 30
Database Selection 15
Device drivers 2
DMI 18
DMI browser 165
  Data Flow 19
  Service 18

E
ECC Memory Service 25
Event Scheduler 42
Events 43
Execution Alerts 9

F
File Transfer 46
firewall 148
Force Remote Logons 9

G
Groups 39, 40

H
Hints and Tips 10
Host Access Definition 153
HTTP 154

I
Installation 3, 117
Installation of
  TME 10 NetFinity Manager 6
  TME 10 NetFinity Services 3
Internet 145
  Browser 146
  CompuServe 149
  Server 147
  Service Provider 149
  Web Manager 151

K
Keywords 8

L
Logs 33
LUN 24

M
Manager 11, 39
Memory 26
Modem Definition 38
Modems 169
Monitor 26
Monitoring 119

N
NetWare 118
NetWare Client 117
Network driver configuration 8
NT Client 117

O
Operating System 117
Operating System Differences 119
OS/2 Client 117

P
passive client 4
PFA 23
POED 47

© Copyright IBM Corp. 1996

Power-On Error Detect 47
Predictive Failure Analysis 23
Process Alerts 35
Process Manager 34
PUN 24

R

RAID Manager 22
Remote Hosts 152
Remote Session 50
Remote System Manager 39, 156
Requirements 1, 146

S

Scheduler 45
Screen View 51
Security 10, 21
Security Manager 20
Serial Connection 36
Service Provider 149
Services 11
Severity 29
Sockets 152
Software Inventory 16
stand-alone client 4
Summary 119
Supported Modems 169
System Information 12
System Keywords 8
System Monitor Service 26
System Partition Access 22
System Profile 15

T

TCP/IP addresses 150
Thresholds 28
Timeouts 9
TME 10 NetFinity functions 11
  Alert Manager 30
  Critical File Monitoring 28
  DMI 18
  ECC Memory 25
  Event Scheduler 42
  File Transfer 46
  Functions 11
  Internet client 153
  Monitor Differences 119
  PFA 23
  POED 47
  Power-On Error Detect 47
  Predictive Failure Analysis 23
  Process Manager 34
  RAID Manager 22
  Remote Session 50
  Remote System Manager 39, 156
  Screen View 51
TME 10 NetFinity functions *(continued)*
  Security Manager 20
  Serial Connection 36
  Software Inventory 16
  System Information 12
  System Monitor 26
  System Partition Access 22
  System Profile 15
  Web Manager 52

U

Utilization 26

W

Web Manager 52, 151
  Browser 146
  Configuration 152
  Internet Connection 145
  Manager 52
  Manager functions 153
  Remote System Manager 156
  Server Sockets 152
  WebFinity 145
Web Manager Functions 153
Webability 145
Windows 3.1 Client 117
Windows 95 Client 117

Printed in U.S.A.